Continuity Planning and Disaster Recovery

Responsible Officer:	AVP - Information Technology Services & UC Chief Information Officer
Responsible Office:	IT - Information Technology Services
Issuance Date:	7/27/2007
Effective Date:	7/27/2007
Scope:	[Scope]

Contact:	Stephen Lau
Email:	Stephen.lau@ucop.edu
Phone #:	(510) 987-0409

I. POLICY SUMMARY

The University is committed to actions that will make campus environments safer and more secure as well as less vulnerable and more resilient in the aftermath of catastrophic disaster or other extraordinary disruption. The President of the University endorsed this commitment by issuing the January 2006 systemwide Policy on Safeguards, Security and Emergency Management.

The purpose of this bulletin is to provide recommendations and guidelines for information technology continuity planning and disaster recovery activities in support of the University's commitment to protection of and accessibility to information resources.

The provisions in this bulletin apply to all University campuses and medical centers, the Office of the President, UC managed national laboratories, and other University locations (campuses) regarding management of its information assets. Certain UC entities, such as UC managed laboratories or medical centers, may be subject to additional federal or state law or other regulations.

Additionally, all academic and staff employees, students, and other Authorized Individuals are responsible for conformance with these guidelines as appropriate to their roles.

II.   DEFINITIONS

Campus
The term "campus" is used throughout this policy in reference to all University locations.

Electronic Information Resources (Resource)
A resource used in support of University activities that involves the electronic storage, processing or transmitting of data, as well as the data itself. Electronic Information Resources include application systems, operating systems, tools, communications systems, data (in raw, summary, and interpreted form), other electronic files, and associated computer server, desktop (workstation), portable devices (laptops, PDAs) or media (CD ROM, memory sticks, flash drives), communications and other hardware used to conduct activities in support of the University's mission. These resources are valued information assets of the University.

Resource Custodian
The authorized University personnel who have physical or logical control over the Electronic Information Resource. This includes, for example, central campus information technology departments with maintenance responsibility for an application; departmental system administrators of a local area network; and database administrators for campus-wide or departmental databases. This role provides a service to the Resource Proprietor.

Resource Proprietor
The individual designated responsibility for the information and the processes supporting the University function. Resource Proprietors are responsible for ensuring compliance with federal or state statutory regulation or University policy regarding the release of information according to procedures established by the University, the campus, or the department, as applicable to the situation. Responsibilities of Resource Proprietors may include, for example: specifying the uses for a departmentally-owned server; establishing the functional requirements during development of a new application or maintenance to an existing application; and determining which individuals may have access to an application or to data accessible via an application. All Electronic Information Resources are University resources, and Resource Proprietors are responsible for ensuring that these Resources are used in ways consistent with the mission of the University as a whole.

III.   POLICY TEXT

A.   *Overview*

The overall goal of continuity planning should be to reduce risk and minimize disruption of campus research and academic programs and of supportive campus business functions. Risk assessments or business impact analyses should be conducted to identify all critical functions of the organization or unit and their supporting information systems. The impact of loss or disruption of functions should be identified, evaluated, and categorized according to the time frames required for recovery of each function

Continuity planning should identify, analyze, and prioritize mission-critical functions based on:
- criticality
- scope and consequences of disruption
- survivability (time-sensitivity)
- coordination requirements with other units or external partners
- facilities, infrastructure, and IT support requirements.

Priorities for response and recovery of academic and business systems should be based on a set of principles defined by the unit or department in conformance with its mission-critical objectives.
Emergency response procedures and disaster recovery efforts should be based on comprehensive impact analyses conducted by teams composed of appropriate administrators, faculty, managers, and information technology personnel as appropriate to the activities of the unit.

B.   Criticality Classification

Resource criticality is a measure of the importance of a Resource to the functional operation of a campus or department and the priority of that function in continuity plans and disaster recovery strategies.
Business and Finance Bulletin [IS-3, Electronic Information Security](#) requires that risk assessments be conducted, and that these risk assessments include an inventory all information resources. Risk assessments should identify the Resource availability requirements according to the criticality and priority status of the information resources. All Resources should be classified into one of the following categories:

      essential to the continuing operation of the University. Failure to function correctly and on schedule could result in a major failure to perform mission-critical functions, a significant loss of funds or information, or a significant liability or other legal exposure.

      necessary to perform important functions. Operations could continue for a short period of time without those functions while normal operations are being restored.

      deferrable for an extended period of time. Operations can continue without those systems or services performing correctly or on schedule.

For more information see [IS-2 Inventory, Classification, and Release of University Electronic Information](#).

Business and Administrative Functions

All campus business and administrative functions supported by information technology should conduct business impact analyses to determine the criticality classification of supporting Resources and their priority for recovery.

Academic Research and Instruction

Risk assessments of Resources that support academic research and instructional activities should be conducted to determine their criticality classification and priority for recovery.

Health Systems

Medical records systems are *essential* systems where regulation requires that they must be available at all times. Risk assessments of any other Resources supporting health-related information should be conducted to determine their criticality classification.

IV.   COMPLIANCE / RESPONSIBILITIES

A. Systemwide

The Associate Vice-President – Information Resources and Communications, Office of the President is responsible for this Bulletin.

The Information Technology Leadership Council, whose members are appointed by Chancellors, medical center directors, and UC managed national laboratory directors, works in partnership with UC academic and administrative leadership to identify systemwide and common campus implementation strategies.

B. Campus

Chancellors, the Executive Vice President - Business Operations at the Office of the President, and UC managed national laboratory directors are responsible for delegating responsibility for implementation of these guidelines at their respective locations. Information Security Officers are responsible for facilitating campus compliance with the campus Information Security Program.

C. Divisions and Departments

Division deans, department chairs, and appropriate administrative officials are responsible for identifying and establishing procedures to achieve departmental compliance with campus implementation.

D. Individuals

All members of the University community are expected to cooperate with campus emergency instructions, follow emergency procedures, and comply with campus policies and procedures in support of this bulletin and to exercise responsibility appropriate to their position and delegated authorities. Each individual is expected to conduct the business of the University in accordance with the [Statement of Ethical]

Values and Standards of Ethical Conduct, exercising sound judgment and serving the best interests of the University.

V. PROCEDURES

Continuity Planning Steps

As required by University policy, emergency preparedness encompasses a set of program elements which are identified by Facilities Administration. Resource proprietors and custodians should ensure that their contingency planning and disaster recovery activities are conducted in coordination with campus emergency planning activities and programs.

Continuity planning at the University of California consists of the following four overlapping phases:

A. Mitigation

Threat events or hazards may be caused by a wide range of technological, natural, human-based or terrorist–related events. A first step in continuity planning requires deployment of protective measures that will safeguard Resources from likely potential harm or loss, or that minimize the extent of impact and duration of disruption.

See IS-3, Electronic Information Security for recommended operational, technical, and physical and environmental controls that should be standard for all information technology-based activities.

Technology Infrastructure
Reliability of the campus technology infrastructure assumes the availability of communication Resources, such as the campus data network and campus telephone and public safety communications systems. Protection and continuity of business functions are achieved by ensuring secure data centers that deploy recommended industry standards.

Essential computing and networking systems must be located in secure, professionally managed data centers that include:
- fire suppression system;
- UPS battery protection;
- back up power system;
- controlled and redundant temperature and humidity environment;
- secure network connectivity, high bandwidth;
- encryption transmission for restricted information;

- system and data back up at a secure, off-site locations that provide standard protection against common hazards, such as fire, flood, earthquake, theft, and decay;
- controlled access to only authorized personnel;
- 7x24 staff availability for monitoring and emergencies;
- secure remote console access from remote location for handling emergencies.

Necessary resources should be located in secure data centers as much as practicable. When alternative locations are selected, they should conform to as many of the elements listed above as deemed appropriate by risk assessments.

Deferrable resources are subject to IS-3 security requirements.

To the extent possible, electronic information should be stored professionally-managed servers rather than on individual desktop computers. System and file back up should be routinely utilized to ensure future recovery in the event of destruction or modification of Resources.

B. Preparedness

Preparedness is critical to continuity planning and disaster recovery. Preparedness involves all of the actions required to establish and maintain the level of capability necessary to implement emergency response plans and conduct disaster recovery operations.

Preparedness is implemented through a continual cycle of planning, training and equipping, exercising, and evaluating and taking actions to correct deficiencies and mitigate vulnerabilities.

Campuses must develop several types of plans, including:
- **Emergency Operations Plans** describe how the campus will respond to any type of emergency or disaster.
- Procedures may include **Standard Operating Procedures**, operations guides, job aids, position checklists, action plans, or other critical information needed for response and recovery.
- **Disaster Recovery Plans** describe the actions to be taken to facilitate both short-term and long-term recovery of resources and campus operational capability.

Plans should recognize the need for flexibility in order to be more responsive to the likely occurrence of unexpected disruptions. Plans should be tested on a periodic basis by various means, such as disaster recovery exercises, testing of alternate sites, or other simulations of potentially predictable emergencies. Plans should be updated to reflect

changing environments, processes, technology, or other impacts as appropriate.

In general, response and recovery plans should include:
- identification of responsible authority to direct emergency response,
- communication plans, in conformance with campuswide communication planning strategies,
- communication alternatives to enable community members to communicate with each other and campus personnel,
- inventory and classification of Resources,
- emergency response procedures, including the specification of teams of personnel assigned responsibility for responding in emergency situations. Planning should anticipate alternative deployment of personnel to address inability of assigned personnel to participate in response efforts,
- communication alternatives to enable team members to communicate with each other and with management during an emergency,
- provisions for equivalent alternate processing in the event of a disaster or other interruption that renders normal processing inoperable,
- provisions for remote worksites,
- deployment procedures to relocate or replicate Resources or facilities,
- procedures that ensure authorized access to back up sites,
- measures to protect vital records or essential data,
- provisions in contracts with external service providers that ensure their preparedness for emergency response and business recovery.

Planning should also consider response to requests from other UC campuses or nearby institutions of higher education that experience emergencies for which they may need additional Resources.

C. Response

Response efforts should follow the pre-planned Standard Operating Procedures and Disaster Recovery Plans. Continuity planning should have determined the priority of activities to address both immediate and longer- term effects of the emergency, including recommended procedures and checklists for action.

Disasters are not predictable, however, and activities may require a resetting of plans, operating procedures, or protocols in response to unforeseen circumstances. If the emergency plan has not adequately addressed the situation, emergency response should rely on the principles and processes established in the planning effort. It is unlikely that initial planning can anticipate all potential circumstances, making it essential that

response teams are prepared to adapt and improvise according to a general outline for recovery.

D. Recovery

The focus of recovery efforts should be on re-establishing operational capability as identified in planning priorities. These priorities may be based on a series of dependencies related to the campuswide emergency response procedures and will vary, depending on the extent of the disruption.

Business continuity

As part of a business continuity planning effort, campus controllers identified a list of business processes *necessary* to conduct University business process in a reliable manner (see Appendix B, List of Identified Business Processes). Of those listed, four business systems are identified as *essential*:

- Payroll/Personnel Systems
- Accounts Payable – Students
- Accounts Payable – Vendors
- Accounts Receivable and Billing – Agency

The controller planning effort was based on the assumption that a generic "business office" had a critical business function for which business continuity was imperative, and that three broad categories would be impacted by an event:

- staff availability
- access to business office physical resources
- availability of central-campus technology infrastructure

For more information, contact your local campus controller's office.

Other departments and units

Managers of academic departments and research institutes/units are responsible for evaluating the impact of likely threat events to their program or function, and should organize recovery according to an established recovery plan, consistent with immediate needs and critical departmental priorities.

List of Identifed Business Processes
(Note: Bolded items selected for planning, assessment)

1. Extramural Funding – Pre Award
2. Extramural Funding – Post Award
3. **Payroll**
4. Health and Welfare Benefits (Verification / Enrollment)
5. Human Resources – Employees

6. Human Resources – Liabilities (taxes)
7. Human Resources – Accounting
8. Human Resources – Hiring, Layoffs
9. Human Resources – Union Negotiations and Changes
10. Human Resources – Time Collection and FCSA
11. Human Resources – Training Records
12. Human Resources – Verification
13. Human Resources – VISA Status
14. **Accounts Payable – Students**
15. Accounts Payable – Employees
16. **Accounts Payable – Vendors**
17. Accounts Receivable and Billing – Students
18. Accounts Receivable and Billing – Housing and Dining
19. **Accounts Receivable and Billing – Agency**
20. Accounts Receivable and Billing – State Claims
21. Accounts Receivable and Billing – Patients
22. Accounts Receivable and Billing – Insurance Claims
23. Card Programs – Purchasing Card
24. Card Programs – Travel and Entertainment Card
25. Cashiering - Access to Money
26. Cashiering – Depositing
27. Cashiering - Reporting
28. General Ledger Maintenance (Includes recharges)
29. Materiel Management – Purchasing
30. Materiel Management – Receiving
31. Materiel Management – Business Agreements
32. Financial Reporting
33. Document Handling - Printing checks
34. Document Handling – Storage
35. Document Handling – Maintenance
36. Document Handling - Records Requests
37. Data Records Management
38. Cash Management – Investments
39. Cash Management – Accounting and Distribution
40. Cash Management – Banking Relationships
41. Cash Management – Wire Transfer
42. Capital – Contracts
43. Annuitants – Retirement Payments, Life Income
44. Benefits – Verification, Enrollment
45. Gifts – Acceptance, Deposits, Restrictions
46. Financial Aid (Separate from A/P, calculations)
47. Budget Systems
48. Data Necessary for State Budget
49. Risk Management – Settlements and Payments
50. Risk Management – Case and Claim Management

> 51.   Risk Management – Workers Comp, Reporting

VI.   RELATED INFORMATION

- [IS-2 Inventory, Classification, and Release of University Electronic Information](#)
- [IS-3 Electronic Information Security](#)

VII.   FREQUENTLY ASKED QUESTIONS

VIII.   REVISION HISTORY

This policy was last updated on July 27, 2007. It was reformatted into the standard University of California policy template on April 20, 2012.