

I&IT Division Business Continuity Plan

Executive Summary

Business continuity planning is about recovery and return to normal business operations after a disaster. The Instructional & Information Technology (I&IT) Division's Business Continuity Plan (BCP) defines how we have prepared for the "return to normal operations" following unexpected emergencies. Since the response is dependent upon the circumstances of the emergency, this plan identifies the critical systems and what we would need to respond, rather than the actual response. The BCP provides a priority order in which services will be restored.

One individual in each I&IT department has been given responsibility for updating their department's section of the I&IT Disaster Recovery Plan, the Incident Kit, and the Business Continuity Plan on a regular basis.

Disaster Recovery Plan

The I&IT Disaster Recovery Plan is part of the overall I&IT Business Continuity Plan and provides the information I&IT will use during recovery efforts to restore and maintain services to the University. This plan assumes that there are staff and managers available with the skills and knowledge about the systems to set them up and maintain them. In the event that there are none available, the campus would need to hire people that have the needed skills set up the systems. This plan is posted in Blackboard and is available for review and use by all I&IT staff.

The plan contains a list of equipment, estimated replacement costs and vendor contact information for all of I&IT's critical equipment. I&IT would need to purchase or repair these items at a minimum to sustain the core technology needs and mission of the University. I&IT maintains an emergency fund of \$1M (\$1,000,000) to pay for this equipment since the university does not carry replacement insurance. I&IT also maintains electronic records for all purchasing and maintenance of the division's critical systems.

Incident Kit

The Projects and Services Manager currently maintains the Incident Kit with input from the division. This kit contains some sensitive information (staff phone numbers) that is not readily available to all I&IT staff. Its main purpose is to have information readily available to all I&IT managers for use during outages, service interruptions and disasters. The incident kit is posted in Blackboard in an area for I&IT managers only. All I&IT managers are directed to keep a current version

of the incident kit files on their campus portable machines or a thumb drive and with them at all times.

Business Continuity Plan

The information contained in the Disaster Recovery Plan and Incident Kit are the key components that make up I&IT's complete Business Continuity Plan. The plan outlines the services that each department in the division is responsible for, how critical they are to the university and information that would be needed to put the service back into production for the university. The plan provides critical contact information and alternate methods for contact in case the normal channels of communication are not available.

How prepared are we?

With all of the information that is maintained by the BCP team, I&IT is well prepared to communicate with each other and our co-location partners (campus technicians who have servers in our computer room) and coordinate the resolution of problems that would arise during an emergency. We are well positioned to determine the severity of the situation and to assess and set priorities very quickly in an emergency. We are also able to quickly procure or repair systems as needed.

I&IT also does periodic BCP exercises and evaluates all unexpected events that occur in to learn and identify ways to be better prepared for future incidents. For example, as a result of the Chino Hills earthquake that occurred on July 29, 2008 I&IT identified that having all I&IT staff and management in Building 98 evacuated by floor was not beneficial for our BCP recovery strategy. We worked with Debbi McFall, who agreed that I&IT should evacuate together in Voorhis Park. The division now knows that B98 I&IT staff are to evacuate to Voorhis Park so we can immediately begin to discuss and evaluate the status of the campus systems together while we are evacuated from the building and begin to develop an action plan for addressing the emergency and its effects on campus central technology services.

I&IT backs up all systems that are located in Building 98 (main data center) to a backup system in Building 1. The backups are then sent off site on a weekly basis. If Building 98 were to become inaccessible, campus data would be restorable from the on-campus backup repository in Building 1 that is kept up to date daily. This will allow us to recover data quickly during an unexpected event. In the unlikely event that both Buildings 1 and 98 are inaccessible, I&IT would be able retrieve campus data from our off site repository. Although this data would be older than the data stored on campus, it would allow us to recover to a point where we could provide the service to the campus relatively quickly once we have the equipment to run it on.

Building 98, where our main data center is housed, has an uninterruptable power supply (UPS) that supports our data center equipment. A generator backs up this UPS. If the campus loses power, the UPS and generator systems would maintain electricity to keep I&IT in the computer room systems operable.

In addition, Cal Poly Pomona uses the CSU's Common Management System (CMS) for all of the student data, financial data and employee records that it maintains. These systems are run from an off site CMS data center in Salt Lake City. If the University was completely inaccessible we would be able to identify a new location to set up systems, restore critical services and support the mission of the University without any disruption to the CMS system or services that it provides.

Conclusion

I&IT maintains a Business Continuity Plan that is robust enough to allow us to quickly obtain critical information that we need to communicate and restore services in an unexpected event. We have worked hard over the years on becoming prepared to ensure that our systems can be quickly recovered in an emergency situation. We have learned and modified our plans when we experienced events that provided opportunities to do so. We also maintain backups in a way that allows the campus to quickly obtain the current data used to supply the campus with services. I&IT is well prepared to handle a variety of unexpected events that would impact the systems that provide IT services in support of the mission of the University.