Business Continuity Planning Guide
For Facilitators Managing Business Continuity Plans

Considerations and Assumptions in Preparing your Plan

As of
June 2, 2010

Prepared by:
Core Life Safety Committee
Table of Contents

I. Overview of BCP..................................................................................................................

II. Business Continuity Plan Purpose and Definition...........................................................

III. Basic Assumptions and Expectations..............................................................................

IV. DU Institutional Planning Strategy...................................................................................

V. Infrastructure Group Assumptions......................................................................................
   1. Campus Safety
   2. Facilities
   3. University Technology Services (UTS)
   4. Risk Management
   5. Communications
   6. Environmental Health & Safety
Overview of Business Continuity Planning

At the University of Denver, a Business Continuity Plan is a departmental-specific plan designed as part of the broader institutional Critical Incident Management Plan (CIMP), for the University. The CIMP is DU’s board-approved response to crisis management and has two distinct processes including pre-incident planning and incident response. See www.du.edu/risk for additional information including the policy and institutional plan. The Core Life Safety Committee is the management group that conducts pre-incident planning and preparedness and is responsible for various functions including Business Continuity Planning for individual departments throughout campus and testing of plans. The Critical Incident Response Team is designated to respond to critical incidents on behalf of the University from an institutional standpoint.

This document is designed to assist you in preparing to build or upgrade your plan, and provide you with basic assumptions that are important to your planning efforts. The basic assumptions are provided from the “Infrastructure” category of departments (see page 5) and intended to be a guide, noting that additional questions may be required specific to your plan.

Business Continuity Planning Purpose and Definition

The Business Continuity Plan is an important program for both departments and responders alike when faced with outages due to various incidents impacting day-to-day operations. When an incident occurs, your pre-planning efforts will help you manage pre-identified critical processes and key essential personnel who may be required to assist the Critical Incident Response Team emergency response and disaster recovery/resumption efforts. Through pre-incident planning, you will have thought through the response and recovery process ahead of time, identifying essential personnel, and workaround procedures that will allow you to continue your critical functions when the usual or customary way of operations may be impacted for a short period of time.

DU Institutional Strategy

When a major incident occurs, the University will typically focus on its core infrastructure operations prior to resuming day-to-day operations. This includes addressing:

a. Life Safety  
b. Reputation  
c. Financial  
d. Operations and Property
The University by means of our Critical Incident Management Plan strives to manage incidents through a broad-based enterprise risk management effort, using best practices and tools to identify, assess, implement, and monitor our activities. Incidents occur in varying degrees of severity requiring varying degrees of response, noting that each incident is a unique event and may require unique response efforts at the time of the incident. Still, we continue to identify those perils and hazards that may create interruptions in normal activities. From there we can review and assess the severity of a potential impact if such an event were to occur, and the likelihood or probability of such an incident occurring. From there, we assess and implement appropriate training based on the impact analysis, and then monitor our efforts and revise them over time as necessary.

Departments Involved in Planning

Our institutional strategy is based on the assumption that those infrastructure departments that are in place to support the institution’s mission may be the very resources that are prioritized to receive primary response and recovery efforts during an incident for the short-term until all resources can be restarted using normal functions. This is in order to recover basic life safety elements that are required in order to provide service to the Key and Other levels. So, in essence, during normal times, Key and Other efforts are priority. During an incident, this hierarchy may be turned upside down for the short-term, in order to get all Key and Other levels back to full service. The level and specifics may vary by incident. The planning table below shows how the organization is divided for planning purposes of response, recovery and resumption.

**Key Operations:** Needed to maintain the University’s critical business or have and impact on safety. These are often academic programs which must have a higher level of maintenance, including research or operations activities to keep the organization running.

**Other:** Basic administration and academic functions that may be moved, continued with workaround plans, or stopped for a short period of time.

**Infrastructure:** Needed to maintain life safety and campus-wide core functions.
### Basic Infrastructure Activities

<table>
<thead>
<tr>
<th>Infrastructure Departments</th>
<th>Primary activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Campus Safety and Transportation</td>
<td>Team Leader for all Critical Incidents, security of site, liaison for local authority, initial investigation</td>
</tr>
<tr>
<td>Facilities Management</td>
<td>Water, electricity, plumbing, central plant</td>
</tr>
<tr>
<td>University Technology Services</td>
<td>Technology including internet, intranet, wireless routers, telephones</td>
</tr>
<tr>
<td>Risk Management</td>
<td>Management of claims and contact with insurers, works with investigators, University Counsel and others in ongoing liability concerns</td>
</tr>
<tr>
<td>University Communications</td>
<td>Manages initial communications for CINS, manages all news media, manages DU Home Page and website blog of incident</td>
</tr>
<tr>
<td>Environmental Health &amp; Safety</td>
<td>Supports CIRT effort as respects life safety, hazardous materials, and other potential concerns</td>
</tr>
</tbody>
</table>

### Basic Assumptions and Expectations of Infrastructure Departments

The following are basic assumptions you can utilize in preparing your plan, provided by the infrastructure departments described above. Should you have any questions, we will provide a contact person for you, and you should coordinate with that individual, or contact the duContinuity responsible person for your area.
Campus Safety

The Department of Campus Safety is the “team leader” in any critical incident. They should be notified in the event of any critical incident that occurs on campus, or is reported from off-site regarding an off-site incident. They are also the key vortex of information regarding incidents, and provide campus safety reports of the incidents to the critical incident response team. In addition, they should be notified when:

- There is an emergency on campus, such as a fire, flood, or other related incident;
- For injuries that occur on campus, or for work-related injuries;
- Any time 911 is called you should also call Campus Safety Dispatch.
- They are also the sender of any CINS messages via phone, email or text.

When an incident occurs Campus Safety will:

- Be the team leader of the incident;
- Provide liaison efforts between DU and local authority (fire, police, paramedics);
- Secure the scene to provide protection of life safety;
- Secure the scene for authorized persons regarding investigation efforts;
- Notify the campus community through CINS, the emergency notification effort;
- Call up the Emergency Operations Center (EOC) if necessary;
- Provide the “all clear” or resume to normal duties confirmation once an incident is complete for major short-term incidents.
  - For longer-term incidents, they will support CIRT efforts which may have rolling resumption/recovery plans.
Facilities Management Infrastructure Assumptions

1) Facilities--Generators
   - We have 12 generators on campus but none of them are designed to operate a building during a power outage. The University does not own a generator that can operate a building. Generators primary purpose is emergency lighting and electricity to safely shut down systems.
   - Generators can be rented to run power for operations of individual buildings but depending on size/load of a building it may take 2-3 days to get one and another 2-3 days to hook it up.

2) Facilities--Power outages
   - Power Outages can be caused due to failure of University equipment but more often than this are due to outages in the Xcel Energy Company system. Xcel is geared up to handle these repairs but their response time is often dictated by how widespread the power outages are. Most outages on campus are typically repaired in 2-4 hours.
   - We have four different power feeds coming into campus so it is rare when the entire campus is without power.
   - Building Outage: It is not unusual to lose part of the power (referred to as single phasing) in a building. This may either be due to a failure of our equipment or Xcel’s equipment. In this case your lights may work but are flickering, your outlets may work, alarm systems will generally show that they are in trouble but still continue to work, however major pieces of equipment (elevators, AC equipment....) requiring 3 phases of electrical power to operate should automatically shut down or be turned off because the equipment can be damaged if it continues to operate without full power.

3) Facilities--Water and Sewer:
   - Water and Sewer outages are less common than power outages. If a building were to lose water/sewer, restrooms can generally be provided in adjacent classrooms and office buildings. The loss of water also affects some AC systems and some heating systems. However, for our Residence Halls, Fisher Early Learning Center, Ricks Center, our event venues and our food service areas these outages can be cause for a facility to be shut down. Like all utility outages, water/sewer outages may be due to a failure in the city’s infrastructure or our infrastructure. These outages although less frequent than power outages are often longer in duration (1-2 days)
4) Facilities--Natural Gas:

- Loss of natural gas is extremely rare on a large scale basis, however, leaks can occur on a smaller scale that will require shut downs of some of our equipment (heating and kitchen primarily).

5) Facilities--Heating or Air Conditioning

- Loss of heating or cooling can be caused by the loss of the utilities mentioned above but also can be caused by the loss of major pieces of heating or cooling equipment or leaks in our underground distribution piping. Depending on size and load temporary equipment can be rented and utilized to get the system running again. Full repairs can take between 1-2 weeks based on the size of the piece of equipment and the availability of similar size equipment in Denver.

- With the exception of large scale utility outages, the loss of heating or cooling is generally on a building by building basis. The University, however, does operate a Central Plant which provides heating for 11 buildings (Shwayder, Sturm, Driscoll North & South, Mary Reed, Margery Reed, Daniels, University Hall, Law, Chambers and HRTM). The cooling operation serves 14 buildings (Shwayder, Sturm, Driscoll North & South, Daniels, University Hall, Law, Chambers, HRTM, Craig, Penrose, UTS, Kappa Sigma, and Lambda Chi). The Central Plant is located in Sturm Hall. Loss of equipment or utilities within the Central Plant will affect all of these buildings.
University Technology Services (UTS) Infrastructure Assumptions

The UTS Disaster Recovery Plan is designed to provide:

1. Institutional Recovery from total destruction of one of its two data centers.
2. The plan also addresses requirements for recovery and continuation in the event that both data centers are damaged or destroyed.
3. In addition, the plan is designed to administer recovery of centrally maintained systems and networks whose integrity or security has been compromised. UTS is currently investigating the feasibility of developing an off-site location for replicating data and/or services in the event of a campus wide disaster.

**UTS--Power Outages and Impact Technology and your plan**

☐ In the event of a power outage, battery-charged laptops will not be able to access the wireless network from a building or location that has no power.

☐ The 2 data centers mirror business critical information and services in real time. Both data centers provide generator power in the event of a power loss. Redundant on-campus networks provide for access to either data center from primary buildings on campus. Each building is wired with Ethernet jacks and most with wireless access points, but building power is required for either of these forms of networking to work.

**UTS--Internet Access from Off-Campus**

☐ At this time, there is only one path to the internet and firewall connections to the external network off-campus. This connection is located in the primary data center. If the primary data center is destroyed, faculty, staff and students will not be able to work from off-campus until the network is rerouted or restored. UTS, is currently investigating the costs of installing a redundant internet connection in the secondary data center.

**UTS--Telecommunications**

☐ The University’s main telephone switch is also located in the primary data center. A secondary telephone switch is located on the north side of campus and allows for a small number of pre-designated lines to be distributed to phones located south of Evans Street. In the event of a loss of the phone switch in the primary data center, campus telephone lines will be capable of recording and retrieving voice mail, but no live telephone use will be available.
UTS--Recovery Sequence

❑ The UTS Business Continuity plan describes the sequence for systems to be restored during the academic year in the event of a large-scale disaster. Any adjustments to the sequence order must be approved by the Vice Chancellor of University Technology Services. The Vice Chancellor will confer with the Chancellor, Provost, and/or Vice Chancellor of Business and Financial Affairs to determine any modifications to the restoration sequence.

UTS--Primary Data Center

❑ In the event of a complete loss of the primary data center, restoration of services will, in some cases, not be immediate. Most administrative business critical services and central academic services will be restored within a few minutes in the secondary data center, but a few may require manual intervention and necessitate a few hours for complete restoration. Non-critical systems may require a few days to a week or longer while substitution of manual operations may be necessary for others. A list of services deemed critical for business continuity is located at the end of this document. Please contact University Technology Services to determine what procedures may be required to bring up a less critical or non-redundant service in the secondary data center.

UTS--Secondary Data Center

In the event of a complete loss of the secondary data center, all central systems will continue to function in the primary data center; however system performance and access times may be slower than usual in some cases. Many colleges and departments house division services and data in the collocation facility, located in the secondary data center. Please contact your college or departmental server administrator for information regarding business continuity procedures for departmental or college services not maintained by UTS.

UTS--Tertiary Data Facility

UTS also utilizes a 3rd data center facility that houses central backups. Backups are performed nightly 7 days/week for data and services that UTS maintains. Data is kept for 1 year. E-mail is backed up for 7 days ONLY for disaster recovery purposes and individual mail boxes or messages cannot be restored except at the request of the Chancellor, Provost or Vice Chancellor.

UTS--Property Destruction

The UTS Business Continuity Plan does not address IT recovery from destruction of any other University offices or facilities. Other departments should work with Risk Management and Facilities to prepare separate plans.
UTS- Redundant Services:  **Timeline: 24-48 hours estimated for recovery**

For BCP Planners: Prepare for up to 4-days without these services noting that recovery is expected to be within 24-48 hours for any major incidents. Extraordinary incidents may take longer.

The following systems are considered to be mission critical and are completely redundant in the data centers. Services must be available within 24-48 hours of loss for the University to continue to conduct business. These essential systems should require little or no downtime to recover in the loss of either data center:

- Campus wide networking and authentication systems (DNS, DHCP, LDAP, Enterprise Active Directory and CaIR domain)
- Campus Voicemail system (Callegra)
- Banner applications including iBanner, myweb, BDMS, and Data Warehouse
- University-wide web services [www.du.edu](http://www.du.edu), mysite.du.edu and Content Management System
- Campus wide electronic mail gateway, centralized mail stores, mailing lists, and webmail
- CaIR Exchange services including Blackberry services
- File and print services for the University administration
- Campus portal (webCentral)
- Blackboard on-line courseware system
- Wireless services
- Cognos Reporting
- duContinuity
- Virtual Hosted systems (UTS and departmental services)

**UTS Services Currently available ONLY in UTS Primary Data Center Facility**

- Campus Internet Connection, Firewall, and external VPN (*currently being evaluated for redundant connection*)
- Campus primary telephone switch
- Blackboard OneCard ID Card system (*currently being evaluated for redundancy procedures*)
- Active Admission system
- Campus Portfolio system (*currently being migrated to redundant services*)
- Campus-wide central printing service
- Ungerboeck scheduling and reservation system
- Campus web-based calendar
- Off-campus modems
- Campus Cable TV connection
- Departmental hosted servers

**UTS-Services Currently available ONLY in UTS Secondary Data Center Facility**

- Departmental housed servers and services in UTS Collocation Facility
Risk Management

Risk Management is responsible for the response and investigation of an incident as respects any potential claims. These claims may include bodily injury claims, property claims, or other claims related to the broad scope of insurance coverage maintained by the university.

Risk Management will work with other CIRT members including but not limited to: The department(s) involved, and University Counsel to manage these incidents on behalf of the University.

Risk Management is responsible for:

- Responding to any incidents to support CIRT efforts;
- Working with other CIRT members to make decisions regarding life safety and protection of property or reputation and protecting the scene for further investigation.
- Fielding any questions or claims filings for the University and providing appropriate response in a timely manner;
- Being the primary liaison between the University’s insurance providers and their representatives and the University-from response through final recovery/resumption.
- Managing any claims that arise from critical incidents throughout their completion and working with any departmental representatives, third party contractors and insurance representatives as needed.
- Can provide pre-planning assistance to departments as requested.
**University Communications**

University Communications (UC) responsibilities are an integral portion of critical incident response, providing the central vortex for information between the University and outside media. Any and all media requests to a university faculty, staff or student should be submitted to UC’s News and Media department. In the event of a critical incident, UC will:

- Providing all official information from the University to the new media;
- Conduct regular updates at a specified “media” center during a large scale event;
- Approve all requests from media to a university official before the official makes comment on a critical incident;
- Manage the institutional communications including providing assistance to Campus Safety Dispatch in sending out CINS messages;
- Manage the updates to the University’s website;
- Manage the critical incident “blog” on the website, posting regular updates on behalf of the Critical Incident Response Team (CIRT).

**Environmental Health & Safety (EH&S)**

Environmental Health & Safety is responsible for all campus responses to hazardous materials spills, EPA or OSHA site visits and interacts closely with the CIRT when needed.

EH&S is responsible for managing:

- For employee workplace fatalities, these must be reported to OSHA within 8 hours of death by EH&S with Risk as a backup if necessary;
- indoor air quality concerns;
- hazardous waste spills;
- OSHA site visits and must be called anytime OSHA arrives on campus for an inspections, site visit, etc. related to University business;
- EPA, CDPHE or other regulatory agencies;
- Other response efforts as required by the incident.