

# **ITMF Disaster Recovery and Business Continuity Committee Report for the UGA IT Master Plan**

## **I. Executive Summary**

Planning for continued operation during unforeseen catastrophic events, and for returning to normal conditions after disruptions, is crucial to the ongoing fulfillment of the University's dual missions of instruction and research. Contingency planning must take into account both disaster recovery, defined as restoration of full operational status after a catastrophe has concluded, and business continuity, referring to continued operation of the University in the event of extended conditions that render one or more buildings or systems on campus, or the residential campus itself, unusable or unsafe. Research provided by the UGA Office of Emergency Preparedness indicates that the major disruptive events most likely to affect the residential UGA campus in Athens, Georgia are major utility failures, structural fires, pandemic flu outbreaks, hazardous materials release, and catastrophic weather events. Worst case disaster scenarios from an IT management perspective include loss of data, extended downtime for critical server-based resources such as IMS and the UGA website, lack of communication tools for coordinating an organized disaster response, and lack of computer facilities for faculty, staff, and students to continue normal University operations for the duration of a disruptive event. The first three scenarios can be mitigated by providing campus with virtual server instances and server hardware hosting in an off-campus datacenter on the Navy School grounds, enabling business continuity in the areas of processing, communications, and data retention. This service offering can also serve as the basis for distributed disaster recovery efforts, maintaining UGA operations at a reasonable percentage of normal effectiveness while replacement equipment and facilities are obtained. This business continuity service can be funded through a hybrid model consisting of central funding in the amount of \$538,000 over five years, augmented by a cost-recovery-based tiered service offering to units and departments on campus. The fourth scenario, loss of teaching, research, and administrative facilities in a building or area of campus, can be mitigated with a standing contingency plan for temporary use of spaces and equipment in the Miller Learning Center.

## **II. Disaster Category Likelihoods**

While the exact probability of events such as tornadoes, earthquakes, and other disruptive events can be difficult to calculate, approximate likelihoods of potential hazards can be gauged for the purpose of determining how to allocate disaster recovery/business continuity (DR/BC) resources. The following chart, provided by the UGA Office of Emergency Preparedness, indicates the rough probability of each of these events occurring at the Athens residential campus:

<b>Hazard/Threat*</b>	Probability HIGH ●	Probability MEDIUM ●	Probability LOW ●
Severe Weather			
Major Structure Fire			
Hazardous Materials Release			
Successful Cyber Attack			
Infectious Disease			
Domestic Terrorism			
Civil Disturbance			
Mass Casualty Incident			
Major Utility Failure			
Earthquake			
International Terrorism			
Active Shooter Incident			

*\* Not in ranked order of probability or likely occurrence. Probabilities and related impacts are based on current trends and similar occurrences in other jurisdictions. Courtesy of UGA Office of Emergency Preparedness.*

Recommendations presented for business continuity preparations will focus on high-probability events in order to make the best use of available resources. For purposes of disaster recovery and business continuity planning with the domain of information technology, it has been determined that “Successful Cyber Attack” can be excluded from business continuity preparations, since the prevention and remediation of this hazard is the primary focus of the Office of Information Security. “Major Utility Failure”, on the other hand, will be addressed, since a local power substation failure is one of a short list of events that could disrupt operations for the entire residential campus.

Two types of disaster scenario, those affecting between one and several buildings and those affecting the entire campus, should be examined when looking at DR/BC preparations from an information technology perspective. Enabling preparation for both types of scenario by providing services and infrastructure to support DR/BC plans is essential to encouraging proper emergency planning by units on campus.

Scenarios involving just one building, or several buildings in a specific area of campus, are of lesser potential impact to campus operations as a whole, but are statistically more likely, and potentially damaging to the operations of the areas affected. The list of emergencies that may affect small areas of campus without directly disrupting the rest of campus includes, but is not limited to, the following:

- Structural Fire
- Hazardous Materials Release
- Weather Event (floods, tornados, lightening)
- Extended local power disruption

Each of the first three scenarios on this list have the potential to destroy computing equipment as well as electronic records, creating administrative problems through the loss of data and server utilities. All four scenarios may render computer workspaces and server-based utilities unusable for an extended period of time.

Several other scenarios exist that, while less likely to occur, would have a much broader impact on the university, potentially affecting the entire campus. This list includes, but is not limited to, the following events:

- Major Weather Event (sustained flooding, multiple tornados)
- Pandemic Flu
- Power Substation Failure (would leave entire residential UGA campus without power)

The first two events on the list could, in extreme cases, make the campus unsafe for occupancy for an extended period of time, which would prevent both use and proper maintenance of computer and server-based facilities. The third event, while not affecting health or well-being of campus occupants directly, could cause computer and server-based facilities on campus to be unusable, impacting both day-to-day operations and longer-term business processes.

### **III. Situation Report**

The UGA Office of Emergency Preparedness and the EITS Office of Information Security have both been successful over the past few years in raising awareness of the importance of DR/BC planning. However, a recent survey indicates that the overall level of disaster readiness of units on campus is not sufficient to ensure prompt recovery and continued operation should a short or long-term disruptive event occur. There is also a high degree of inconsistency in the degrees of implementation and effectiveness of these measures.

The survey indicates that out of 43 responding departments, only 25% currently have offsite backup arrangements in place for critical data, defined as secure locations off-campus where copies of backup media or the backup data itself can be stored. Additionally, only 30% of responding departments currently have DR/BC plans in place. While units on campus are aware of the necessity for these plans, several factors have been identified that may be getting in the way of compliance with this necessity:

- Expense of redundant systems, offsite storage, etc.
- Security concerns regarding non-UGA offsite facilities
- Lack of UGA controlled off-site storage and redundant server facilities

Uncertainty over justification for funding, how to implement DR/BC measures, and what constitutes secure storage of UGA data, may be impeding progress in this area. Additionally, the expense of setting up individual arrangements for each department on campus may be difficult to accommodate, particularly for smaller departments.

## **IV. Recommendations**

Recent surveys have indicated among campus units a high level of interest in complying with institutional mandates regarding the planning and implementation of disaster recovery and business continuity strategies. Measures such as provisioning an off-campus DR/BC datacenter at the Navy School, identifying the MLC as an emergency workspace, and identifying alternative off-campus academic and research computing resources are recommended in order to aid campus units in overcoming the identified barriers of expense, security concerns, and lack of availability of UGA-controlled facilities for redundant server installations.

### **Off-Campus DR/BC Facility in Navy School Datacenter**

In order to ensure the availability of critical communications utilities that can be used to coordinate emergency responses, as well as the continuation of UGA business operations in the event of extended disruption on campus, it is recommended that the University implement off-campus data backups and off-campus server facilities in the Navy School datacenter. This service offering can be funded through a combination of central funds for the initial infrastructure development and personnel, and cost-recovery service offerings to fund maintenance and upgrades. This plan will leverage economies of scale to provide campus units with affordable services from which to develop their own DR/BC plans, and will reduce wasted resources, duplication of effort, and potential data security problems by eliminating the need for each unit to develop separate DR/BC solutions.

The Navy School location is recommended due both to proximity to campus and sufficient distance from it, to exclude it from probable damages from any of the list of disasters likely to affect the residential campus. The Navy School area is powered by a different power substation than the main campus, reducing the risk that one power failure will affect both areas. The distance also decreases the probability of catastrophic weather events affecting both datacenters adversely. While a failover datacenter located further away might mitigate a broader list of disaster categories, such as pandemic flu outbreaks, the University is better off with regard to security if redundant data storage and servers are housed in a nearby location controlled by the University, rather than a distant location controlled by an external party.

Implementation of this plan will require some additions to the server infrastructure at the Navy School datacenter. A redundant secure storage array with a capacity of 100 terabytes, costing approximately \$185,000, will provide sufficient space for the initial implementation of DR/BC and central backup services that will be offered to campus departments, and will ensure data preservation and integrity should the Boyd Datacenter be compromised by fire, flood, or power issues. Five hardware servers for the housing of virtual redundant servers, which will be used as failover systems for UGA departments that use this facility for DR/BC measures, will cost around \$53,000 for the initial deployment. A total of one full-time-equivalent support position, costing approximately

\$60,000 per year, will be sufficient for facilities management and monitoring and for server and backup system administration.

The cost-recovery service offerings will consist of three service tiers. The first tier, consisting of hosting facilities for client-owned hardware, will provide off-campus redundancy for clients whose servers cannot be virtualized, or who prefer to provide their own hardware for other reasons. The second tier, virtual servers for “warm” failover capacity, will consist of virtual server instances housed on the server hardware mentioned above, which will be periodically updated with client data, and can be activated in the event of extended downtimes on campus. The third tier, virtual servers for “hot” failover capacity, will provide for mission-critical services that need to be constantly available, with up-to-the-minute data synchronizations to maintain data integrity. Clients will be charged for these services based on power usage, disk capacity needed, and frequency of data synchronization, so that funding for facilities maintenance, systems monitoring, and staffing requirements will scale with the total usage of the services. Based on this model, the lowest usage tier will be available to clients for approximately \$116 per month, rendering this DR/BC solution affordable even to the smallest units on campus.

### **Alternative Academic and Research Computing Resources**

While contingency plans have been put in place or are being implemented for providing redundant servers for business services such as the student record system, the UGA webserver, eLearning Commons, and other mission-critical systems, less attention has so far been given to academic computing activities such as research. Grid computing consortia such as SURAGrid can be used for the continuation of research-related processing, in the event that use of the research computing infrastructure housed on the UGA campus becomes unavailable. It is strongly recommended that redundant resources for academic computing be identified, and that research computing concerns be made a part of the current DR/BC awareness efforts on campus.

### **Provisioning the MLC as an Alternative Workspace**

In a scenario where one or more buildings on campus are rendered unusable for an extended period of time, office space and access to computers might become a limiting factor for the affected campus units with regard to maintaining business processes. While some departments already have contingency arrangements for alternative workspaces, over half of those areas surveyed responded that they would be interested in a centrally arranged alternative workspace. The Miller Learning Center is a good example of a facility that might be identified in advance as an alternative workspace for temporarily displaced campus units. Putting an alternative workspace plan in place will provide additional options for departments working to complete their DR/BC strategies.

## V. Solutions in Use by Peer and Aspirant Institutions

Ensuring that institutional units maintain continued operations, or resume operations in an expedient manner, and that disruptive events are effectively managed and mitigated, is a crucial element of emergency planning for colleges and universities. The following describes disaster recovery and business continuity approaches currently being used or implemented by several comparator peer institutions and aspirational peer institutions of the University of Georgia:

**The University of Texas at Austin** offers virtual server creation and maintenance as a client-paid service through their Information Technology Services division. These virtual servers run on hardware that is located in a secure physical location and is monitored 24/7. All servers are backed up weekly, and the service is provided to the UT Austin community as a disaster recovery solution.

**The University of Arizona** maintains an off-campus data center for backups and disaster recovery. This redundant datacenter is connected to the primary datacenter by a high-speed fiber link, enabling whole virtual servers to be transferred back and forth in order to provide load-balancing services in addition to disaster recovery instances of critical services.

**The University of Wisconsin at Madison** has implemented several redundant datacenters in various locations around the city of Madison, Wisconsin, linking them with high-speed connections to enable split-second failover capability in the event of outages or disruption at one location. Departments are encouraged to virtualize computing resources, both for easy disaster recovery and for saving power to support green technology initiatives.

**The University of Florida** has virtualized all centrally-managed servers, and is in the process of building an off-campus datacenter to serve as a mirror site, enabling both load-balancing and business continuity with instant failover capability. Virtual server hosting is offered as a cost-recovery service to campus units, with pricing based on server type and desired capacity.

**Cornell University** offers server hosting services on a cost-recovery basis, in a datacenter complex spanning two campus buildings. High-availability configurations for disaster recovery, business continuity, and improved speed of access are provided, and off-campus redundant hosting is offered for mission-critical systems. The CIT office works with campus units to implement these configurations in support of disaster recovery and business continuity policies.