CUNY
Business Continuity and Disaster Recovery
Task Force

Information Technology
Subcommittee

IT Disaster Recovery/Business Continuity Recommendations

Adopted by CUNY IT Steering Committee on September 16, 2010
Adopted by CUNY BC/DR Committee on October 18, 2010

Prepared by:

Sehgal, Varun – Chair

Anderson, Scott (BMCC)
Argiropoulos, Chris (CUNY Law)
Cammarata, Carl (CIS)
Campbell, Robert (Grad Center)
Cohen, Brian (CIS)
Downing, Arthur (Baruch)
Gold, Mark (Brooklyn)
Haggard, James (CIS)
Kress, Mike (CSI)
Lader, Wendy (CIS)
Panchal, Praveen (John Jay)
Uddin, Rita (City Tech)
Tighe, Peter (York)
## Contents

Introduction .................................................................................................................................................. 3

Initial Recommendations .............................................................................................................................. 5

Data Protection and Recovery ...................................................................................................................... 6

I. Periodic Data Backups................................................................................................................................ 7

II. Disaster Recovery Planning ..................................................................................................................... 10

II-a. Conduct a business impact analysis ................................................................................................... 10

II-b. Develop disaster recovery/business continuity plans ........................................................................... 12

III. Proactive Loss Prevention ..................................................................................................................... 13
Introduction

The City University of New York (CUNY) is a very large and complex institution, serving hundreds of thousands of students, employees, and alumni. It operates virtually non-stop throughout the year and is bound by contract with its customers, by New York State and Federal Education guidelines, and by New York State and Federal Financial Aid rules, to provide specific services within specific timelines to meet expectations. CUNY’s customers depend on it to be able to meet their expectations and any significant interruption of operations has the potential to create substantial problems, including economic, scheduling, educational standards, human capital, and credibility.

As with any enterprise of this size, CUNY is extremely dependent on information technology systems and IT infrastructure to provide needed services and maintain required records. Of course, IT is only one component of a wide variety of systems and resources that underpin the CUNY enterprise, and which must be considered in comprehensive planning to ensure business-continuity and recovery from possible disasters. However, IT is probably one of the more fragile components, depending as it does on so many electrical, environmental, and technical resources, which are so easily disrupted, and it therefore should be in the forefront of an organization’s consideration of how disasters can disrupt their operations.

Every unit of CUNY has an obligation to apply industry best practices to protect its records, keep its operational systems running and accessible to users, and support its instructional and research activities, with the least possible interruption. This obligation is based on contractual, fiduciary, statutory, and even moral obligations to students, employees, alumni, government funding organizations, granting organizations, and more.

IT Business Continuity and Disaster Recovery

Business Continuity and Disaster Recovery in the IT space encompass a very wide range of activities and plans that generally speaking try to address the following:

- Minimize the likelihood of critical IT systems and services failing
- Speed the restoration of failed systems or services, or have alternative processes ready to be implemented
- Protect the integrity, security, and accessibility of institutional data and records
- Prevent irretrievable loss of critical records, including archival records mandated by law to be retained based on pre-defined schedules

This document addresses a variety of IT Business Continuity and Disaster Recovery best practices that should be adopted as quickly as possible by all operational units of CUNY, including all colleges and the CUNY Central Office organizations. The guidelines, suggestions, and standards, included in this document have been drawn from industry standards, and adjusted to meet CUNY’s “business models”, as well as CUNY’s generally more-limited financial resources. They include both “bare minimum” actions, as well as more comprehensive recommendations for enhanced protection and recoverability.

While many CUNY units have implemented very advanced BC/DR practices, there are significant portions of CUNY that lag behind even the most basic protections. The goal of this document is to help bring all CUNY units up to minimally acceptable levels of BC/DR standards, and to encourage continued
improvements that can be implemented as CUNY-wide initiatives – sharing costs and resources to make them as affordable as possible.

**Governance**

The IT BC/DR Subcommittee that prepared these recommendations is a part of the CUNY-wide BC-DR Task Force, which seeks to educate the University about the need for wide-ranging BC-DR planning and to encourage that planning. This document will become a part of the Task Force’s larger recommendations, but will also be promulgated through the University’s IT Steering Committee, which has authority to approve and recommend CUNY-wide IT best-practices and standards.

It is important to note that the IT specialists at each CUNY unit are the appropriate responsible parties to coordinate IT BC-DR enhancements and standards at their organization – even for infrastructure not under their direct control. However, recommendation II involves a wide range of business units and divisions at each CUNY unit. These recommendations are included in this document because IT BC-DR is usually inextricably bound with those processes and IT is typically more sensitive to the challenges that make BC-DR planning imperative. However, IT does not have the authority, resources, or business knowledge to manage these discovery and planning processes for the entire campus. These efforts will only be successful with strong executive buy-in at each CUNY unit, the assignment of knowledgeable key personnel from each business unit (including faculty), and the designation of an overall coordinator to manage the work.

**Planning for IT BC-DR**

Although some initial recommendations for immediate implementation will be made below to address some of the most critical and urgent needs, each CUNY unit must begin the more involved process of analyzing its mission-critical IT systems, and planning how each critical system, process, and data source will be protected; how the institution will ensure that its business operations can continue in the absence of those systems, processes, and data; and how the failed components can be restored to full operation.

Basic general steps are described below. They will likely involve resources, input, and planning not only from IT, but from all of the offices, functions, and constituents that depend on IT’s services and facilities. CUNY may also opt to retain outside experts to guide and coordinate these efforts. The needed analyses, the creation of reliable effective BC-DR plans, and the culture changes required to ensure that the plans can be “activated” on short notice, may take quite some time to complete. It is recommended that CUNY approach the analyses by functions, and begin to address each portion of the analysis as they are completed.

**Common Practices = uniform common planning = reduced costs**

While CUNY’s various units are different in many ways, they also have many aspects of their operations that are similar, if not identical, to one another. This creates opportunities to define solutions that can be shared by multiple institutions, and to benefit from the likely cost savings resulting from joint procurement of any needed BC-DR services, systems, or facilities. We recommend that CUNY centrally coordinate the analyses of the common systems and functions, to facilitate faster implementation of suitable IT BC-DR initiatives across CUNY units.
Furthermore, the CUNYfirst implementation will require all colleges and many other central units to closely examine how their primary mission critical processes affect offices unit-wide. This presents a unique opportunity to leverage that discovery process to also meet IT BC-DR analysis goals.

**Initial Recommendations**

The BC/DR IT Subcommittee proposes the following recommendations, which are detailed in subsequent pages. These represent the most critical high-level needs that must be addressed as quickly as possible. Many CUNY units are already in compliance with at least recommendations I and III, but few, if any, have completed II.

As each unit progresses towards meeting minimum standards for data protection, loss prevention, and disaster recovery, the University will be in a position to recommend or mandate further levels of security, protection, and recoverability, as resources permit.

I. **Periodic Data Backups:** That all CUNY units make periodic backups as described below under “Periodic Data Backups”. Specifically, units must take steps to store backups at the unit in secure, protected facilities; must use an off-site storage facility to store backup sets updated at least weekly; and include in the backups all mission critical data, especially instructional materials, financial transactions, student records–related information, etc; and maintain appropriate documentation for procedures implemented. Please note that the examples supplied of typically critical systems are a general recommendation. Each unit must seriously consider the level of criticality of each dataset, analyze what would be required to recover from the loss of that data, and plan for an appropriately frequent backup schedule and a suitable number of redundant backup sets. Prioritization of DR/BC planning for mission critical systems (wherever they may be found on campus) is based on a variety of factors including availability of appropriate resources. The subcommittee strongly suggests that this recommendation be targeted for implementation within six months across all CUNY units.

II. **BC Risk Analysis and Disaster Recovery Planning for CUNY Units:** That CUNY retain consulting expertise to work with the IT BC-DR committee to create an overarching set of plans and guidelines to guide CUNY units in the required self-analysis of risk levels, available risk mitigation steps, disaster recovery plans, and business continuity plans. It is recommended that outside consulting resources and dedicated CUNY resources be assigned to assist CUNY units to complete the necessary plans on a rolling basis over the next two years, with the most mission critical functions given priority. The subcommittee suggests that this recommendation be targeted to initiate implementation within six months and be completed within two years. (*Please note important governance considerations noted on page 4 above)

III. **Proactive Loss Prevention:** That all CUNY units ensure that the infrastructure hosting its data and applications be equipped with at least basic features described below under “Proactive Loss Prevention”, such as RAID storage, redundant power, UPS backup, etc.

   a. That all CUNY units ensure that future acquisitions of servers, storage devices, and other active components be equipped as recommended.

   b. That CUNY units running mission critical applications and services – especially online services – on equipment not sufficiently fault tolerant, or in facilities not sufficiently optimized to protect central IT systems, consider budgeting for upgrades and replacement with all due haste to address that serious deficiency.
Data Protection and Recovery

Every organization captures and stores electronic records of all sorts, such as emails, web pages, student information, vendor information, accounting records, research data, student assignments, course information, etc. In fact, with the increasing penetration of online data gathering, electronic workflows, and e-signatures, it is not uncommon for critical data to exist only in electronic format, having never been recorded on a paper form or report. Even records that begin as paper records can easily be damaged and should be electronically archived in case of paper loss. Loss of critical data could result in: a student being unable to prove that he/she earned a degree, the university being unable to determine who owes the institution money or who is owed money by the institution, or an instructor having to assign course grades without access to their notes, online grade book, or student submissions. These are just a few examples of possible major consequences of data loss or long-term data unavailability.

Much of the data captured and stored by CUNY have statutory requirements for records retention, which mandate that the university ensure that the information be available for retrieval for a specific number of years – sometimes indefinitely. CUNY has published very comprehensive schedules of what information needs be retained, and for how long. Those guidelines include electronic records, and each unit must consider those requirements when planning their backup cycles.

The task of data protection is to ensure that both data accessed regularly in normal operations (such as current student records, A/P, A/R, etc.), as well as archival records, are secured from unauthorized access and damage, protected from loss, and duplicated in backup or archival copies that can be retrieved in case of loss or corruption.

Of the three recommendations that follow, Periodic Data Backups (I) and Proactive Loss Prevention (III) begin to address CUNY’s obligations to safeguard its data. Periodic data backups are addressed as the first priority since proactive safeguards against loss are capital intensive and may take longer to implement. During that period it is critical that CUNY at least ensure that its units can recover from the inevitable data losses that result from equipment failure, accidental damage, and environmental disasters.
I. Periodic Data Backups

Storage systems fail; data gets corrupted; users make data entry mistakes; records get wrongly and irretrievably altered due to errant software or inappropriate access privileges; data integrity gets compromised due to security failures; data centers become inaccessible. These are just some examples of the numerous reasons why it may become necessary to restore data from a backup, and it is basic required business practice to ensure that all data is backed up on an appropriate schedule and stored in safe locations that can survive threats to the primary storage systems.

How Backed up?

Data backups can be accomplished by a variety of means and software tools, but the tool selected should have at least the following capabilities:

- Be capable of backing up “live” applications with open files
- Be capable of securing the resulting backup files with password protection or encryption
- Be capable of restoring data to alternate media, servers, etc.
- Be capable of processing a variety of needed file systems (Unix, Windows, Apple, ...)
- Have enough market penetration and installed base to make it likely that it will be continually upgraded to new systems platforms and remain supported to retrieve older archives
- Be capable of creating full, incremental, and disk-image backups.

For backup operations that will require multiple media to store the backup, an automated multi-item library is strongly recommended so that backups can proceed without manual user intervention. Backups sometimes encompass enough data to make it difficult to back up the target data during an off-peak time window. One solution to this problem, is creating a hierarchy of storage, where data is first backed up quickly during off hours to an active storage device such as a NAS or SAN, and then backed up to tape from that secondary device during working hours. This not only enlarges the backup time window, but also provides a near-term backup resource from which recent files can be restored without resorting to offline media.

How Often?

Data backups must be refreshed on a regular schedule that factors in the size and complexity of the dataset, the frequency of changes, the ease of recreating it, the severity of the impact on operations caused by the process of backing it up, and many other factors.

Optimally, mission critical systems data - i.e. data for systems that are not easily recreated, and which can cause extreme disruption when they fail – should be backed up more often, preferably also in real-time to a parallel storage system. Less critical data, or data that changes more slowly and less often, could be backed up less frequently.

At minimum, CUNY units should ensure that:

- Data supporting mission-critical systems are backed up completely (master backup copies) weekly and incremental backups (including just changed records) daily. Examples: Student records, student coursework and submissions, email or email transaction logs, financial transaction logs, in-process online applications or service transactions.
• Less critical data are backed up weekly, or at least monthly. Examples: logs of non-financial and non-registration type transactions, mostly static web page content.
• Archives of old records need only be created initially and only updated when the archive is updated. Multiple copies should be maintained in disparate locations.

What Storage Medium?

Backups can be stored on:
• Magnetic tapes (although some magnetic media must be refreshed periodically and may not be suitable for very long term archiving purposes)
• Portable disk systems
• Remote active storage systems (SAN’s)
• CDs/DVD media
• Portable solid state memory systems
• Any combination of these and other similar media

Whatever the medium, a rotating set of at least grandparent, parent, child backups should be maintained. In the case of time-critical data, a series of file snapshots may be appropriate at various incremental dates in the records lifecycle.

Stored Where?

CUNY units must store, and update regularly, at least one set of all data backups at an off-site facility designed to safeguard critical business data, such as Iron Mountain or GRM. The off-site facility must be a secure, environmentally controlled facility that regularly houses such data and is as far away from the unit location as possible without compromising the ability to retrieve backup media quickly when needed. Off-site backup vendors must be prepared to commit to a suitable service-level agreement for pickup, management and return of off-site backup media as requested by the unit. In particular, the off-site backup facility must be able to deliver requested media back to the unit within 4 hours of a retrieval request. The means utilized to pick-up and deliver the media must meet security and privacy standards, and the data itself should be secured and/or encrypted by the CUNY unit to prevent disclosure. The storage facility and the delivery/retrieval processes must ensure that the data is protected in conformance with statutory requirements, such as FERPA, HIPAA, Fair Credit Reporting, etc.

Backup media stored offline locally in the unit’s own facilities must be stored in a secured cabinet or safe specially designed to protect sensitive magnetic media for a reasonable period of time from damage in the extreme heat of a fire, or the corrosive effects of a flood. CUNY units that have ready access to locations within their organization that are significantly distant from the data sources (such as other buildings on a campus,) should consider storing rotating sets of backup media there.

Testing and Validating

Offsite backups should be recalled periodically to verify the CUNY unit’s ability to successfully retrieve backup media, as well as to verify that the offsite backup provider can successfully meet their delivery promises.

Test restorations of backup datasets (regardless of storage medium) must be made periodically – both to an alternate file location, as well as to the original location. These tests validate the integrity of the backup process, as well as ensure that the CUNY unit is prepared to restore backups when required.
Summary:

Required: Periodic backups to multiple sets of removable media
Better: Periodic backups to secondary active storage and then to removable media

Required: Storage of media in environmentally secure enclosures within the unit
Required: Storage of rotating backup media sets in a secure off-site storage facility
Better: Storage of additional rotating backup media sets in a remote location within the unit

Best: Real-time backup to parallel storage and server systems in secondary location, preferably at least 50 miles away
(This is an additional backup and cannot replace regular off-site media backups)
II. Disaster Recovery Planning

In order to be functionally prepared to operate in, and recover from, a disaster that impacts IT or functions dependent on Information Technology services, it is paramount that CUNY and its various campuses prepare a formal IT Disaster Recovery Plan. The requirement of this plan is also important to successfully pass various audits to which CUNY IT and the campuses are subject to. The two major tasks associated with the development of a disaster recovery plan are outlined below.

II-a. Conduct a business impact analysis

Each CUNY unit must review and document those IT services, applications, tools, systems, infrastructure (equipment, telecomm, software, etc.), and even human capital that underpin each major critical operational function. Some examples are: registration, billing, purchasing, computer labs, email, web sites, smart classroom systems, grade collection, archival records access, admissions processing, etc.

Certainly the most critical functions, and the functions that are most IT dependant, should be considered first. Campuses may find that the loss of some IT functions have very little impact, either because they are rarely used, can wait for systems to be resurrected, or because there are very simple manual alternatives to the IT processes. Other functions may be nearly impossible to maintain in the absence of the IT systems that support them. It is important to consult widely to properly gauge the effect of a failed system or data loss. Note that seemingly unrelated offices and functions often come to depend on systems that were not designed with them in mind.

While each CUNY unit needs to make its own determination as to the relative importance of each function to its operations, most organizations consider at least the following to be critical - not only because they are heavily used by all constituents, but because they become even more critical during an IT disaster, when the ability to communicate electronically is most needed:

- Phone systems
- Email and related systems such as Blackberry Servers
- Internet access infrastructure
- Web sites and Portals

Similarly, most colleges would consider at least the following functions to be critical for at least parts of each term:

- Admissions processing
- Registration
- Billing and payment processing
- Financial Aid processing
- International Student, NY Residency, and Immunization verification and processing
- Grading
- Attendance
- Testing
- Course Management tools
- Library electronic resources
- Computer Labs and smart classroom systems
Ironically, the more sophisticated a unit is in using IT systems to facilitate these functions, the more critical it is that the unit plan for failures.
II-b. Develop disaster recovery/business continuity plans

Some examples of issues to consider when developing plans:

- Consider what steps can be taken to minimize the likelihood of the identified function failing. How can the underlying systems be made more redundant? Can backup systems be prepared and made accessible quickly in case of an outage?
- Can the function be relocated away from an environmental problem that is causing the systems to be unavailable?
- How could the function be temporarily accomplished without the benefit of automation or access to electronic records?
- Does the unit ensure that backups are made regularly of the affected electronic records so that reasonably up-to-date copies can be retrieved quickly to support a restored system?
- How accessible are the people who know how to manage, operate, and correct the systems? Are there alternate staffers, or outside consultants who can fill their shoes if they become unavailable or incapacitated?
- Is there a ready location away from the affected area where IT operations can be resurrected? Does that location have the minimally required equipment, software, and telecomm access?
- How will all of the proposed plans be tested? Under what circumstances will they be activated and what steps are required to do so? How will we ensure that these tests do no impact operations during or post-testing?

These are just a few of the important questions that each unit must ask in developing effective plans and systems to ensure business continuity.
III.  Proactive Loss Prevention

Although some data loss may eventually be inevitable, there are some basic precautions that CUNY units should be utilizing to reduce the likelihood of data loss and system interruption. These system features should be included in the specifications of any new infrastructure that is acquired, and should be retrofitted where possible into the existing infrastructure.

**Cooling:** Servers and storage devices should be housed in temperature controlled facilities and in well ventilated rack or cabinet systems. Vents and equipment enclosures should be kept dust-free. HVAC systems that serve these spaces should be at least partially redundant so as to allow the equipment to survive a loss of cooling power for an amount of time that would give the unit an opportunity to safely shut down devices and possibly repair the cooling systems. Standby standalone high-volume cooling fans should also be stored nearby to mitigate a loss of cooling in an emergency.

**Electric:** All mission critical devices should have redundant power supplies (preferably N+1). Those power supplies should preferably be fed from disparate electrical circuits. Mission critical devices should also be backed up by uninterruptable power sources – either a central UPS system, or individual UPS’s serving individual devices or cabinets. Optimally the UPS systems should be further backed up by a diesel generator, although this is a costly and high-maintenance feature that may not be practical or affordable for many CUNY units.

**Access:** Mission critical devices, including network equipment in closets throughout the campus, and certainly server and storage farms must be secured from unauthorized access. If possible, network equipment should not share space with unrelated equipment, such as security, AV, or telecom equipment, unless they can be segregated securely one from the other.

**Media:** Storage disks should be replaced on a regular cycle well before their probable end of life. The same goes for servers and other mission critical devices with active mechanical components. Some server monitoring systems have predictive failure warnings (E.G., HP SMART) for storage devices and media that should be monitored regularly.

**Redundancy and fault tolerance:** Servers and storage systems must have their storage configured in a RAID array – at least RAID 1 mirroring, but preferably RAID 5, and in high-availability situations RAID 6 or 10. RAID controllers should preferably have a battery-backup feature.

**Servers:** Servers should preferably have ECC memory that can survive minor errors, and multiple CPU’s that may survive a single CPU failure. Server systems that consolidate multiple server applications using VM machines, or servers-on-a-card should be planned to spread application support across multiple systems so that the failure of any one server has the least possible effect on high-availability applications.