The College actively participates in the CUNY Disaster Recovery and Business Continuity activities. Vice President Michael Kress and Victor Magnani are members of the sub-committee. CSI will follow the lead the University provides to develop a plan for Disaster Recovery and Business Continuity for technology infrastructure.

**Purpose**

The purpose of this plan is to offer a guide to recovery of critical IT systems and restoration of service in as timely a manner as possible in the event or disaster.

**Scope**

At present the plan focuses on IT systems that are under the purview of CSI OTS.

**Summary**

A detailed document (DR plan) containing specific instructions for recovery of critical systems, along with contact information for staff and vendors, is maintained by the Office of Technology Systems. Copies of this plan are held by key personnel in OTS.

**Declaring Disaster**

For the purposes of this plan, a disaster can be considered anything from damage to the physical space (fire/flood) to systems failure. Any extended interruption of critical business systems would fall under this plan. Critical systems are monitored 24/7 and once notified personnel will investigate to determine if failure is quickly recoverable or rises to the level of disaster declaration. Should it be worthy of declaration, upper administration officials should be notified. Contact information and chain of contacts is outlined in DR plan. Determination would be made as to informing CSI population (students, faculty, staff) via email, web notification or other means possible of outage and estimate of return of service. Details for recovery of individual systems are contained in the DR plan and are reviewed, updated and tested regularly.

**Contents of DR plan**

- Details of backup/restore procedures for systems covered under plan
- Contact information for CSI staff
- Vendor information for key hardware/software services
- Contact information for CUNY CO

**During Disaster**
There is no hot-site for CSI to adjourn to in case of disaster. It is unlikely that the entire campus would become unusable, so relocation within the campus would be probable course of action if location of critical system hardware became unavailable. There is a hosted web site, collegeofstatenisland.info, which would provide outlet for emergency messages in case campus infrastructure was unusable. Instructions for accessing and updating this hosted site (which is usually a redirect to CSI homepage) are included in DR plan.

Instructions for recalling backups stored off-site are also contained in the DR plan. Only authorized personnel may call for these backups to be returned.

It should be noted that a number of critical systems have some level of failover implemented, some automated, some requiring intervention. These are tested along with other aspects of DR plan.

CSI staff should be in close contact with CUNY CO staff in case changes made during recovery need to be reflected via CUNY CO across the internet. All relevant contact information for CUNY is contained in DR plan.

After Disaster

Once it is possible to stand down – either because of permanent or temporary restoration of systems and/or services – this status should be communicated through to the administration following the same flow as when disaster was declared. A decision can then be made as to informing the wider CSI community of the status.

A review should be conducted as soon as feasible and any lessons learned should be incorporate into future drafts of the plan.