CUNY Bronx Community College
DEPARTMENT OF INFORMATION TECHNOLOGY

DISASTER RECOVERY PLAN

Revision 3 - 7/3/2014

TABLE OF CONTENTS

OBJECTIVES

The primary objective of this Disaster Recovery Plan is to help ensure the continued operation for BCC by providing the ability to successfully recover computer services in the event of a disaster.

Specific goals of the Plan relative to an emergency include:

1) To detail the correct course of action to follow,
2) To minimize confusion, errors, and expense to the organization, and
3) To effect a quick and complete recovery of services.

Secondary objectives of this Plan are:

1) To reduce risks of loss of services,
2) To provide ongoing protection of company assets, and
3) To ensure the continued viability of this Plan.

OVERVIEW

This Disaster Recovery Plan is a comprehensive document containing the necessary instruction, policies, organization, and information required for the BCC to be prepared for an emergency that would affect our computer services. The Plan consists of seven major sections.

Section 1 -- Emergency Response Team
Section 2 -- Emergency Control Center
Section 3 -- Critical Applications
Section 4 -- Contingency Site
Section 5 -- Recovery Procedures for a Major Disaster
Section 6 -- General Procedures for Potential Interruptions
Section 7 -- Backup Policies
Section 8 -- Testing and Maintenance of the Plan

The following is a brief description of each of the seven sections of the Plan:

SECTION 1 - THE EMERGENCY RESPONSE TEAM

Described in this section is the organization responsible for constructing and maintaining the Disaster Recovery Plan, for managing the disaster recovery activities, and for the continued viability of the Plan.

SECTION 2 - THE EMERGENCY CONTROL CENTER

This section includes a detailed description of the facilities to be used for managing and coordinating activities in the event of a major disaster.

SECTION 3 - CRITICAL APPLICATIONS

Included here is a table illustrating the BCC's critical applications and the current administrative liaison assigned to support them.

SECTION 4 - CONTINGENCY SITE

The contingency site is detailed. This section includes a description of the facilities provided and all requirements associated with the use of the site.

SECTION 5 - RECOVERY PROCEDURES FOR A MAJOR DISASTER

Instructions and procedures to be followed in the event of a major disaster are described in this section. Included are activation of emergency procedures, establishment of computer operations at the contingency site, and subsequent restoration of normal operations

SECTION 6 - GENERAL PROCEDURES FOR POTENTIAL INTERRUPTIONS

Potential, non-major interruptions of service are described and general instructions for handling each type of interruption are provided. Typical interruptions include fire, power outage, and telecommunications failure.

SECTION 7 – BACKUP POLICIES

Included in this section are policies defining how and when mission critical information is backed up and how to recover it in the case of a major disaster.

SECTION 8 - TESTING AND MAINTENANCE OF THE PLAN

This section contains the policies and procedures needed to ensure that the Plan remains viable as the business environment evolves.

SECTION 1 – EMERGENCY RESPONSE TEAM

1.1 PURPOSE

The purpose of the Emergency Response Team is to establish and direct plans of action to be followed during an interruption or cessation of computer services caused by a disaster or lesser emergency. As the name implies, the Emergency Response Team maintains readiness for emergencies by means of the Disaster Recovery Plan. The Emergency Response Team is also responsible for managing the disaster recovery activities following a disaster, and can be thought of as the "disaster management team". The Emergency Response Team will consider protection of property and business continuation in all phases of the Plan.

1.2 ORGANIZATION AND PLANNING

The Emergency Response Team consists of an Emergency Coordinator and the Action Team Leaders. In the case of a major disaster the Emergency Coordinator will manage the execution of the disaster recovery plan (according to the procedures in Section 5 of this document) from the Emergency Control Center. Action Teams will facilitate the Emergency Coordinator and respond to the various types of emergency situations. The Emergency Coordinator will administer the Plan. The following organizational chart defines the Bronx Community College current Emergency Response Team. **Appendix A** details contact information for the Emergency Response Team and the Action team members.

EMERGENCY RESPONSE TEAM

- **Emergency Coordinators**
- **Applications Team Lead**
- **Communications Network Team Lead**
- **User Support Team Lead**
- **Engineering Team Leads**

The following is a description of the roles and responsibilities of the Emergency Coordinator and the Emergency Response Teams.

1.3 EMERGENCY COORDINATOR

The Emergency Coordinator is responsible for developing and coordinating the Action Teams. During an emergency situation the Emergency Coordinator will activate and then direct all activities until the emergency is under control. Additionally, the Coordinator is responsible for the following:

- Participate in the evaluation and updates of the Disaster Recovery Plan to assure that all emergency situations have been adequately considered and that appropriate contingency plans have been prepared.
- Ensure that the Emergency Response Team and other employees receive proper training of emergency plans and procedures. This will routinely be done as part of an annual review of the disaster plan. The Coordinator will also work with departmental managers to ensure that new employees are properly trained and that certain emergency procedures are reviewed as frequently as necessary.
- Keep all members of the Emergency Response Team fully briefed on all aspects of the disaster plan.
- Evaluate the readiness and proficiency of each Emergency Response Team member and the appropriateness of their assignments.
- Keep management informed of the status of the Emergency Response Team and the Disaster Recovery Plan.
- Communicate the status of emergency situations to management promptly and efficiently.

BCC has three Emergency Coordinators. The three Emergency Coordinators are the Chief of Public Safety, the Chief Information Security Officer and Chief Technology Officer.

**The Chief Technology Officer is the Business Owner of the Disaster Recovery Plan.*

1.4 THE ACTION TEAMS

The following Action Teams have been defined for use in disasters or major emergencies. The purpose and responsibilities of the Action Teams are described on the following pages. The Teams will be activated selectively by the Emergency Coordinators and/or the Emergency Response Team according to the nature of the emergency. The Action Teams report to the Emergency Coordinator during an emergency or major disaster.

- Action Teams
- Applications Team
- Communications Network Team
- User Support Team
- Engineering Team

Designated leaders of the Action Teams and their contact information are identified in Appendix A.

1.4.1 APPLICATIONS TEAM

PURPOSE: The purpose of the Applications Team is to ensure proper functioning of the applications and to coordinate with users about how their applications should be operated during the contingency period.

RESPONSIBILITIES:

- In an emergency, the Applications Team must participate in preparation and validation of the production environment at the contingency site. If problems are identified with how an application will operate at the contingency site, the Applications Team must prepare and document solutions for the problems.
- Coordinate with end-users to determine work that was in progress at the time of the disaster. When operations are restored at the contingency site, the Applications Team must first help recover any lost work that was in progress.
- Once production capability has been recovered, coordinate with the users to synchronize the work done on the disaster recovery systems with the new production systems.

1.4.2 COMMUNICATIONS NETWORK TEAM

PURPOSE: The Communications Network Team is responsible for all shared network systems, as well as, repair or replacement of all lines and associated communications hardware, and its installation and testing.

RESPONSIBILITIES:

- Participate in the evaluation and selection of contingency site(s), testing at the contingency site, and all hardware-related contingency planning.
- In the event of a disaster, assess the extent of damage or the affect of failures on data and voice networks.
- Coordinate with vendors in obtaining necessary repairs or replacement of hardware.
- Coordinate with Purchasing, Finance, Insurance, and other departments in equipment salvage, insurance claims, and financing for replacement equipment.
- Install and test all new/replacement electronics or data lines, and supervise all problem solving when problems or failures are encountered.

1.4.3 USER SUPPORT TEAM

PURPOSE: The User Support Team is responsible for all desktop considerations related to problem calls during a disaster. This includes providing information about the status of services and alternatives.

RESPONSIBILITIES:

- Participate in the evaluation and selection of all desktop hardware-related contingency planning.
- In the event of a disaster, assess the extent of damage or the affect of failures on desktop computers.

- Install and test all new/replacement desktop hardware and supervise all problem solving when problems or failures are encountered.

1.4.4 ENGINEERING TEAM

PURPOSE: The Engineering Team is responsible for the operating system and application software for all Application servers.

RESPONSIBILITIES:

- Participate in the evaluation and selection of contingency site(s), testing at the contingency site, and all hardware-related contingency planning.
- In the event of a disaster, assess the extent of damage or the affect of failures on server hardware.
- Coordinate with vendors in obtaining necessary repairs or replacement of hardware.
- Coordinate with Purchasing, Finance, Insurance, and other departments in equipment salvage, insurance claims, and financing for replacement equipment.
- Install and test all new/replacement server hardware, and supervise all problem solving when problems or failures are encountered.

SECTION 2 – THE EMERGENCY CONTROL CENTER

In the event of a major disaster, the Emergency Control Center will be established from which all communications and activities will be directed. The Control Center will be used to coordinate the management of recovery procedures, and will serve as the center of all communications between the Emergency Coordinators, the Action Teams, and all other personnel.

The Emergency Control Center will contain two sites. The primary site is located in the President's Conference Room suite #17 within Language Hall. The direct phone number to reach the primary Control Center in the event of a disaster is 718.289.5148. The secondary site will be located in South Hall suite # 109 Conference Room. The direct phone number to reach the secondary Control Center in the event of a disaster is 718.289.5929.

The administration of the Emergency Control Center is the responsibility of the Chief Information Security Officer.

- The Emergency Control Center will be activated by the Chief of Public Safety or the Chief Information Security Officer or Chief Technology Officer when a major disaster has occurred, especially when the personal safety of employees or property is jeopardized. Direction of activities and communications with the Action Teams from the Control Center is the responsibility of the Emergency Coordinator.
- This center will provide centralized and coordinated control of communications during emergencies. When the Emergency Control Center is in operation, the Emergency Coordinator and Action Team Leaders will coordinate with the center and keep it informed of status and progress.
- If conditions warrant closing of facilities, the Emergency Control Center will communicate the closing notice through the management chain to all employees.

SECTION 3 - CRITICAL APPLICATIONS

The following tables list the major IT enterprise systems and the critical applications that will be available from the contingency site in the case of a major disaster. Additionally, the assigned Information Technology (IT) staff members and end-user are listed. IT staff are critical members of the Applications Action Team. Detailed contact information for IT staff and the end-users is listed in Appendix A

FINANCIAL RECORDS SYSTEM – MAJOR APPLICATIONS & RESPONSIBILITIES

1. SQL Databases

HUMAN RESOURCE SYSTEM – MAJOR APPLICATIONS & RESPONSIBILITIES

1. HCM
2. HR Timesheet
3. SharePoint
4. PersonalDataForm
5. BCCPersonalDataForm
6. BCCTelephone

STUDENT INFORMATION SYSTEM – MAJOR APPLICATIONS & RESPONSIBILITIES

1. OSSES
2. ASAP
3. Adult and Continuing Program
4. SharePoint
5. CER
6. BIOCF
7. HRAPPS
8. HelpDeskInquiry

MEMBERSHIP INFORMATION SYSTEM – MAJOR APPLICATIONS & RESPONSIBILITIES

1. Active Directory
2. FIM

ADMINISTRATIVE INFORMATION SYSTEM – MAJOR APPLICATIONS & RESPONSIBILITIES

1. Parking Decal
2. Duplicating System (DRS)
3. Campus Event Registration
4. BCCCalendar
5. BCCWakeOnLan
6. BCCwebAdmin
7. BIODemo
8. CER

9. MailTracking
10. RSVPAdmin
11. TSCSurvey
12. BCC Website

COMMUNICATION INFORMATION SYSTEM – MAJOR APPLICATIONS & RESPONSIBILITIES

1. OSSES
2. Exchange Mail System
3. Phone System

SECTION 4 - CONTINGENCY SITE

4.1 LOCATION

The contingency site housing the disaster recovery systems is located in Colston Hall 800

4.2 FACILITIES

The contingency systems consist of a warm site for major IT enterprise application systems.

Collectively, this equipment will house and serve the administrative applications that are mission critical to the institution.

Additionally, there are databases and domain servers. Databases servers are used to house reports and data output from the enterprise systems and the domain servers other act as domain controllers for authentication. Lastly, there are DHCP, DNS, and LDAP servers located in the contingency site to provide necessary directory and networking services.

SECTION 5 - RECOVERY PROCEDURES

The following contingency plans are for use in a major disaster. That is, a disaster of serious enough magnitude to require the computer processing to be moved to the contingency site.

PROCEDURES:

5.1 NOTIFICATION OF THE EMERGENCY RESPONSE TEAM

A critical aspect of disaster recovery is the quick reaction of the Emergency Response Team. This requires immediate notification of appropriate personnel so that the Disaster Recovery Plan can be initiated as quickly as possible.

The Emergency Coordinator has established and will maintain an Emergency Notification List (see Appendix A) and will ensure that all key personnel have it available. In the event of a disaster, the following notification procedures will be followed:

1. If the disaster occurs while IT staff is on duty, they should initiate the notification process as soon as possible. If IT staff is NOT on duty, the Chief Information Security Officer will contact the Emergency Coordinators.

2. The Emergency Coordinator is at the top of the Notification List. If the Emergency Coordinators cannot be reached the next named person on the Notification List will be called until a member of the Emergency Response Team has been notified.

5.2 INITIAL EMERGENCY RESPONSE TEAM PROCEDURES

Once the Emergency Response Team has been notified, they must proceed to make an immediate assessment of the situation and to initiate appropriate actions.

PROCEDURES

1. The first member of the Emergency Response Team notified is responsible to notify other critical members of the Emergency Response Team and to initiate action. The initial action will be to assemble the team at the Emergency Control Center.

2. If the Emergency Coordinator has not yet been reached, the persons listed next on the Emergency Notification List will assume full responsibilities of the Emergency Coordinator, until he or she has arrived and been fully briefed. The Emergency Coordinator or acting Coordinator will proceed to implement the contingency plans.

3. Make an assessment of the situation directly at the scene if possible, or if not, indirectly based on reported information from the notification sources.

4. Based on the Team's assessment of the situation, determine the severity of the problem and decide on the appropriate action.

5. If the emergency is not regarded as a major disaster, then the appropriate correction or contingency plans will be implemented. In such case, selected Action Teams may still be required and will be notified to take action.

These steps constitute activation of the contingency plans for a major disaster. Additional procedures are provided on the following pages for these tasks.

5.3 ACTIVATION OF THE EMERGENCY CONTROL CENTER

In the event of a major disaster, a centralized control center will be established from which the Emergency Coordinators can direct all communications and activities.

PROCEDURES:

1. The Emergency Coordinators are responsible for maintaining an Emergency Control Center in a state of readiness. The Control Center is equipped with table(s), chairs, telephones, marker boards, flip charts, communications, etc.

2. If necessary, telephones will be ordered from the telephone company for emergency installation, and supplies obtained from backup or other sources to properly equip the Center.

5.4 NOTIFICATION OF ACTION TEAMS AND TOP MANAGEMENT

In the event of a major emergency, Action Teams and top management of the organization will also be notified and apprised of the situation. Top management needs to know about the emergency and the current status of personnel, property, and so on. The Action Teams are intended to carry out very specialized functions in a disaster recovery situation, and will be called in to act according to the emergency.

PROCEDURES:

1. Determine which Action Teams should be activated and if the presence of any top management is required to support the emergency activities or contingency procedures.

2. In notifying top management, inform them briefly of what has happened, the current status, the plan of action, and the location and phone numbers of the Emergency Control Center. The Emergency Coordinators should inform the executives whether their presence is required and when.

3. In activating the Action Teams, the Team Leaders of each required team will be called from the Notification List in Appendix A. Inform them briefly of what has happened, the current status, the plan of action, and the location and phone numbers of the Emergency Control Center. Each Team Leader has the Disaster Recovery Plan at home and is expected to be prepared to initiate action appropriate to his/her Team. He or she is responsible for notifying the team to assemble and act according to their contingency plans.

5.5 SUMMARY OF PROCEDURES FOR CONTINGENCY OPERATIONS

This section provides an overview of contingency operations.

SUMMARY OF PROCEDURES

1. The Emergency Response Teams will assemble at the Emergency Control Center for briefing, discussion of any identified problems, and coordination of the contingency plans.

2. The Applications Team will proceed to identify the work in progress that needs to be recovered and how that can best be accomplished. The Applications Team will go to the contingency site to help bring up the applications and recover work in progress. They will be responsible for notifying the user departments and coordinating their interface procedures.

3. The Engineering Team will proceed to the contingency site immediately and begin loading software and data to prepare for computer operations. Once established, processing will be maintained at the contingency site as long as required.

4. If hardware has been destroyed, damaged, or negatively affected, the Engineering Team will proceed to take the appropriate contingency measures to repair or replace the affected hardware.

5. The Emergency Coordinator will continue to maintain the Emergency Control Center as long as appropriate, and will coordinate the contingency operations until they can be returned to a normal, non-emergency state.

5.6 PROCEDURES FOR REPLACEMENT OF DATA CENTER

If the data center is destroyed, steps will be taken immediately to establish a replacement data center. A location must be found with adequate space; computer rooms must be

constructed or modified; and computers, air conditioners, power distribution equipment, raised flooring, cabling, etc., must all be obtained and installed to prepare a working data center.

PROCEDURES:

1. If equipment or facilities are salvageable, the Emergency Coordinators and the appropriate Action Team Leads will assess what is usable or repairable and what needs to be replaced. They will initiate all salvage, relocation, and repair activities as necessary.

2. The Emergency Coordinators will initiate ordering of all new replacement equipment and facilities on an emergency (rush) basis. Financial, legal, and insurance issues will be dealt with in this process.

3. The Communications and Engineering Teams will coordinate with the Physical Plant on all construction issues, including obtaining permits, installation, wiring, etc., to ensure that the data center is properly prepared.

4. The Engineering and Applications Teams will test the readiness of the new data center.
5. When it is ready, they will transfer operations from the contingency site to the new data center.

6. The procedures will be complete when all problems with the new data center have been resolved and operations have been normalized.

SECTION 6: GENERAL PROCEDURES FOR POTENTIAL INTERUPTIONS

A series of procedures follow as a reference for prompt and appropriate actions to be taken in potential emergencies or events that cause interruption of computer service.

6.1 CONTINGENCY PLAN FOR FIRES

6.1.1 PREVENTION

- Review all areas of responsibility for combustible material.
- Operational areas are to be sight checked by each shift before they leave, and particularly if area is to be left unoccupied. Periodically inspect below raised floors. Floor panel lifters are located in the computer room operations area.
- Education of the staff: new employees with access to the equipment room will be educated about the fire plan. The location of exits, location and proper use of extinguishers, location of fire alarms, operation of wet pipe system, etc. will be reviewed with each employee by their respective supervisor.
- The Department of Public Safety, upon request, will perform site inspections which include a general area review, and checks of electrical connections, fire extinguishers, and smoke detectors.
- Periodic inspection and testing of the fire alarm system is performed by the company contracted for the service and the Department of Public Safety.
- Smoking is not allowed in any area within the building.

6.1.2 DETECTION

- The Computer Room has a fire detection and suppression system. Smoke detectors are located on the ceiling and below the raised floor. If smoke is detected, horns will sound inside and outside the computer room. A zone detection panel is located in the main Computer Room which is linked to the building alarm system which indicates the alarm condition. The Computer room detection system, connected to the building alarm system, will automatically send the alarm to the Dispatcher monitor station and, if multiple zones are detected, will activate the wet pipe fire suppression system.
- Detectors and fire extinguisher are also located in areas around the perimeter of the room.

6.1.3 PROCEDURES IN THE EVENT OF A FIRE

- If the fire is small, use a fire extinguisher. Pull the pin on the fire extinguisher, and then discharge the extinguisher by aiming at the base of the fire using a side-to-side sweeping motion. Call Security to inform them of the condition so inspections can be performed.
- If there is a fire and no alarm has sounded notify Security at 718.289.5923 or extension 5923 and pull the emergency fire alarm switch at each building entrance.

6.2 CONTINGENCY PLAN FOR ELECTRICAL POWER OUTAGES

The data center is protected by uninterrupted power supplies (UPS) which will support operations during most brief routine power outages. UPS battery backup provides sufficient power to maintain operations for up to 20 minutes. A emergency generator provides the capability for extended operations should power be interrupted for more than 10 minutes. Prior to the installation of this generator, systems should be shutdown in the proper order when there is an extended power disruption.

6.3 CONTINGENCY PLAN FOR NETWORK FAILURES

All networking infrastructure/communication equipment in the data center is covered by maintenance. Core routers, switches, and network communications servers serve both the data center and multiple components of the organization network, backbone, internet connections, and the users. The cable plant supporting communications to the network equipment is placed in protective sleeves, termination boxes, or conduit. This is made up of both fiber optic and copper cabling. The station cabling supporting connectivity to the file servers, mainframe, user workstations, and network communications servers, are customized.

- In the event of a partial disaster, every effort will be made to determine the scope and severity of the failure or outage and report to the appropriate action team leader. On hand temporary replacement parts or re-routing of data services will be provided until the appropriate replacement parts become available. In the event that the cable plant has been compromised, a joint effort between Network Services and the Physical Plant must take place to provide the necessary re-routing, splicing, or temporary replacement of cabling until a more permanent solution can be achieved. In some partial disaster scenarios, a combination of both temporary equipment and cabling will be necessary. Every effort will be made to restore service as quickly as possible with all available coordinating parties involved.

- In the event of a major disaster with the data center possibly being destroyed, re-routing of cabling services and network infrastructure will be required. The necessary replacement equipment and temporary patch/plug cabling will be required. Equipment in alternate sites would be reconfigured to carry the network traffic. As long as the main backbone cable plant entry point (located Colston 318), or the pathway from it to the data center has not been compromised, the reconfiguration of off-site equipment will provide minimum data service within 48 hours of dispatch. If the data center has been compromised, damaged, or destroyed, the provisions for utilizing a "mobile recovery room/vehicle" will be necessary to provide cable plant "junctions" to bypass portions of the core building cable plant. Network infrastructure equipment under maintenance or off-site equipment provided by the disaster recovery vendor will replace damaged, destroyed, or compromised equipment and possibly run communications out of this facility. The appropriate action team leaders will make the decisions on the viability of this facility or vehicle. Every effort will be made to provide minimum data service with the above structures in place within 72 hours of dispatch.

In both partial and major disasters, having the infrastructure equipment in close proximity to the servers, network services communications servers, and other key organization servers and services that currently reside in the data center or any of the systems replaced due to disaster, is key to reliable network and data service recovery.

6.4 CONTINGENCY PLAN FOR FLOODING

6.4.1 PREVENTION

- It is the responsibility of Facilities Management to be aware of, and consult with Operations Management, relative to the risks of flooding with respect to the Data Center.
- Facilities Management should know where water pipes and drains are in respect to the Data Center, and to know what the potential is for flooding from above (upper floors or roof).
- Facilities Management may periodically arrange for inspection of all pipes and valves within the Data Center for leaks.

6.4.2 DETECTION

The detection of water within the Data Center, particularly under the raised floors, is vitally important to prevent electrical shocks, short-circuits, or equipment damage. The Data Center has under-floor water detectors located at key places around the room.
These devices will emit an intermittent high-pitched alarm when activated.

6.4.3 EMERGENCY PROCEDURES FOR FLOODING

- Invoke the emergency call list immediately.
- If flooding is such that there is no risk of electrical shock, computer operators and engineers should invoke emergency power down sequences for the system(s) before cutting power. Otherwise, computer operators should leave the area immediately.
- All power is to be shut off to equipment before evacuation. In the Data Center, emergency power off (EPO) switches are located at each exit. Either of these switches will cut off all power to the equipment in the computer room. There is a "Drop Load" button on the main UPS unit in the New Hall 25 that will disconnect power to the distribution panel. Additionally, there is a power off button for the UPS.
- If time allows, do all that is possible to provide for the protection of the equipment. If flooding is coming from the underground wall, open the drain plug in the hall leading to janitor room and use carpets as a water block to prevent entry into the computer room. When water is expected due to weather conditions, Physical Plant Services may provide sand bags to create barriers to prevent water from entering under the room doors. A wet/dry vacuum is located in the stock room to assist in removing water.
- If flooding is such that employees should evacuate the building, notify the Physical Plant Services or the Department of Public Safety immediately.

6.5 CONTINGENCY PLAN FOR HARDWARE FAILURES

In most circumstances, the hardware can be repaired sufficiently quickly to restore operation within several hours. Even if the downtime was as long as a day, the preferred approach is to allow the engineers to make their repairs in the normal manner. Hardware failures generally require either repair or replacement.

6.6 CONTINGENCY PLAN FOR SOFTWARE FAILURES

Operating System software is typically under maintenance from the vendor. In the event of a system failure, Systems Engineers and Operations will work to determine whether the failure is hardware or software related. If the failure is software related, Systems Engineers will work with the Vendors technical support staff to correct the problem in a timely manner. Normal restart procedures will often circumvent the problem temporarily until the investigation is completed and resolution is reached.

6.7 CONTINGENCY PLAN FOR APPLICATIONS FAILURES

Most of our applications packages were purchased from third-party sources and are maintained by those companies. Some were developed or highly customized and are now maintained by our Applications Development staff.

Applications software is very similar to systems software as far as failures of new versions of the programs. In-house change control procedures provide for adequate testing before making changes and for backing out the changes if problems are detected. However, a more serious type of application failure is one where, through error of a program, a user, a maintenance programmer or other means, data is caused to be incorrect to the degree that business consequences are serious.

In this case, the programming staff who supports the failed application must determine how the erroneous data will be corrected, with possible assistance from the application software vendor. Backups of data files on tape may or may not be useful depending on the amount of time elapsed during which the error proliferated. In serious cases, special-purpose programming may be required to repair the data. In the worst case, the original source transactions will be re-input in order to rebuild the data files, after correcting the programs and removing the erroneous data.

SECTION 7 – BACKUP POLICIES

7.1 PROTECTION OF COMPUTER DATA

Computer data is protected by a combination of backup procedures and off-site storage procedures. Backups copy the data from disk to removable media (usually magnetic tape) so data that is lost or damaged for any reason can be restored. Off-site storage for magnetic tapes (or other forms of information) protects the data in the event that the computer itself is destroyed due to a disaster in the Data Center.

7.1.1 WINDOWS SYSTEMS

Software: *Symantec Backup Exec 2014*
Hardware: *1-Dell Power Edge R510 with Dell PowerVault TL2000 Tape Library. One drive is directly connected to Group, one directly connected to Netapp and two are for other backups and duplication. See Appendix B for more details.*

All Other Servers

A full backup is performed every Monday with 3-week retention.
A cumulative incremental is run every weekday except on Monday's with 1-week retention. See Appendix B for more details.

Catalog Backups

The catalog gets backed up after every backup. The catalog is duplicated and vaulted each week with the vault job. The vaulted catalog is retained for 1 week. See Appendix B for more details.

SECTION 8 - MAINTENANCE OF THE PLAN

8.1 POLICIES AND PROCEDURES

The effectiveness of the contingency plan is impacted by changes in the environment that the plan was created to protect. Some major factors, which will impact the plan, are new equipment, changing software environment, staff and organizational changes, and new or changing applications.

The following policies and procedures have been developed to ensure that the Plan is reviewed and updated on a regular and reliable basis.

PROCEDURES:

- The Chief Technology Officer will periodically appoint a review team of one or more people to review and update the Disaster Recovery Plan.
- When the review team has completed their review and update process, the Emergency Coordinator will also review and approve the revised Plan.
- In conjunction with the process of review and update of the Plan, the Emergency Coordinator will design, schedule and notify team members of the annual review. The

test may vary from year to year, in order to evaluate different elements of the Plan, but at the least it must address all major procedures involving all teams and must test the ability to process at the contingency site.

- The Emergency Coordinators will ensure that plan-holders receive the revisions to the Plan.

- More frequent reviews/updates of the Plan may be initiated by the Emergency Coordinators, but shall require the approval of the Chief Technology Officer because of probable impact on other projects.

- Testing of the Plan will occur

APPENDIX A EMERGENCY CONTACT LIST

EMERGENCY IT RESPONSE TEAM

Role, Name, (w) Phone # (c) Phone

Emergency Coordinator
James Verdicchio # (w) 718-289-5922 # (c) 718-640-4206
Jonathan Lacay # (w) 718-289-5752 # (c) 917-796-7536
Loic Audusseau # (w) 718-289-5168 # (c) 347-563-3484

Applications Team Lead
Deira Pereyra # (w) 718-289-5777 # (c) 917-502-3499

System Team Lead
Alan Mei # (w) 718-289-5771 # (c) 347-920-7308

Network Communications Team Lead
Augusto Reyes # (w) 718-289-5771 # (c) 917-270-7179

User Support Team Lead
Helen De Jesus # (w) 718-289-5776 # (c) 646-832-8457

Engineering Team Lead
Errol Williams # (w) 718-289-5107 # (c) 917-816-4732

ADMIN APPLICATIONS TEAMS
Deira Pereyra # (w) 718-289-5777 # (c) 917-502-3499
Derrick Le # (w) 718-289-5782 # (c) 917-232-8351
Sammy Henry # (w) 718-289-5774 # (c) 917-817-6872

FINANCIAL DATABASE RECORDS SYSTEM APPLICATIONS TEAM
Deira Pereyra # (w) 718-289-5777 # (c) 917-502-3499
David Ling # (w) 718-289-5224 # (c) 917-952-4992

STUDENT INFORMATION SYSTEM APPLICATIONS TEAM
Deira Pereyra # (w) 718-289-5777 # (c) 917-502-3499
Derrick Le # (w) 718-289-5782 # (c) 917-232-8351
David Ling # (w) 718-289-5224 # (c) 917-952-4992

HUMAN RESOURCES SYSTEM APPLICATIONS TEAM
Deira Pereyra # (w) 718-289-5777 # (c) 917-502-3499
Derrick Le # (w) 718-289-5782 # (c) 917-232-8351
Sammy Henry # (w) 718-289-5774 # (c) 917-817-6872

MEMBERSHIP INFORMATION SYSTEMS TEAM
Alan Mei # (w) 718-289-5771 # (c) 347-920-7308
Carlos Rodriguez # 718-289-5100 x5049 # (c) 917-327-3930

APPENDIX B BCC DISASTER BACKUP IMPLEMENTATION PLAN

OVERVIEW

BCC is part of one of the 25 colleges of The City University of New York (CUNY) and as a requirement and best practice of any large organization and institution we might preform precaution alternatives and plan for any disaster to arise while ensuring all data is recoverable. As a continued effort on data protection, Bronx has implemented a backup system running Symantec Backup Exec 2014 to protect our data as well as sending backup tapes out to a 3rd party data retention company for storage.

The Objective

- Rebuild any critical systems failure
- Protect and minimize critical data being loss
- Ensure continuous business functionality

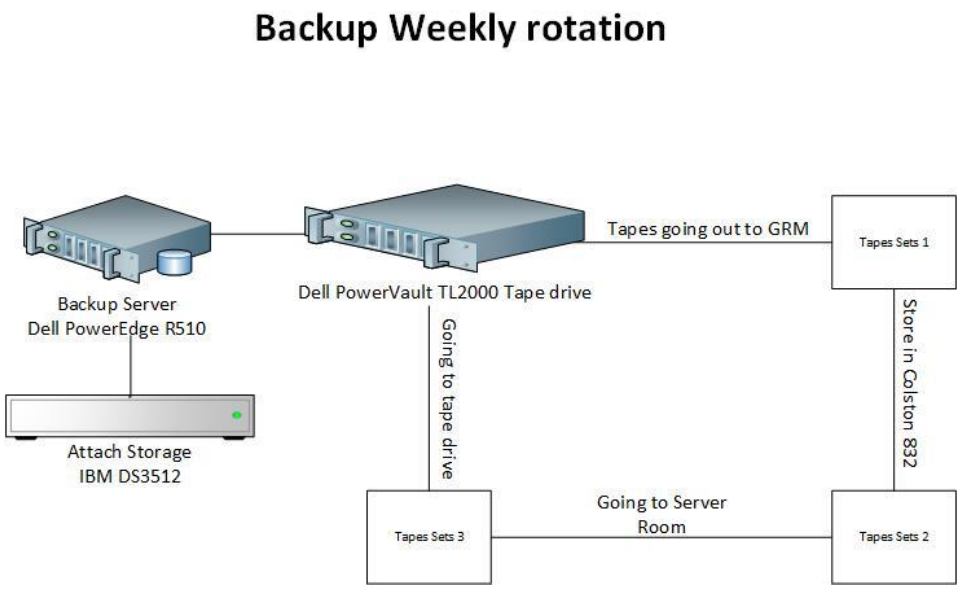
OUR BACKUP SYSTEM

Over the years, Bronx has relied on Symantec Backup Exec to protect data. Our backup system consist of one Dell PowerEdge R510 server, one IBM DS3512 attach storage and one Dell PowerVault TL2000. Backups are scheduled every week, with a full backup on Monday and an incremental from Tuesday to Friday on a local storage, followed by an immediate backup to tape media. Backups are overwritten every week with 3 sets of tape rotation. Each set contains 8 tapes with GRM Document Management coming to pick up on a weekly basis. The 3 sets of tapes consist of 1 set in the PowerVault TL2000 located at the New Hall Datacenter, latest copy going to the vendor and 1 set at the Colston Hall Datacenter.

SERVER SPEC

Device	CPU	Memory	Disk Space
Dell Power R510	2 - E5520 @ 2.27GHz	12GB	6.17TB
IBM DS3512	N/A	N/A	18.1 TB
Dell PowerVault TL2000	N/A	N/A	4GB uncompressed 8GB compressed tape

Backup Weekly Rotation Diagram



Systems/Servers Backup List

Description	Full Backup	Incremental
Email System database	Monday to Friday	None
Registrar Imaging System database	Monday	Tuesday to Friday
Bcc-baud	Monday	Tuesday to Friday
Bcc-image	Monday	Tuesday to Friday
Bcc-it02	Monday	Tuesday to Friday
Bcc-it03	Monday	Tuesday to Friday
Bcc-it05	Monday	Tuesday to Friday
Bcc-libweb	Monday	Tuesday to Friday
Bccsms	Monday	Tuesday to Friday
Bcc-testing02	Monday	Tuesday to Friday
Bcc-web	Monday	Tuesday to Friday
Cfcs01	Monday	Tuesday to Friday
Dcs01	Monday	Tuesday to Friday
Eds01	Monday	Tuesday to Friday

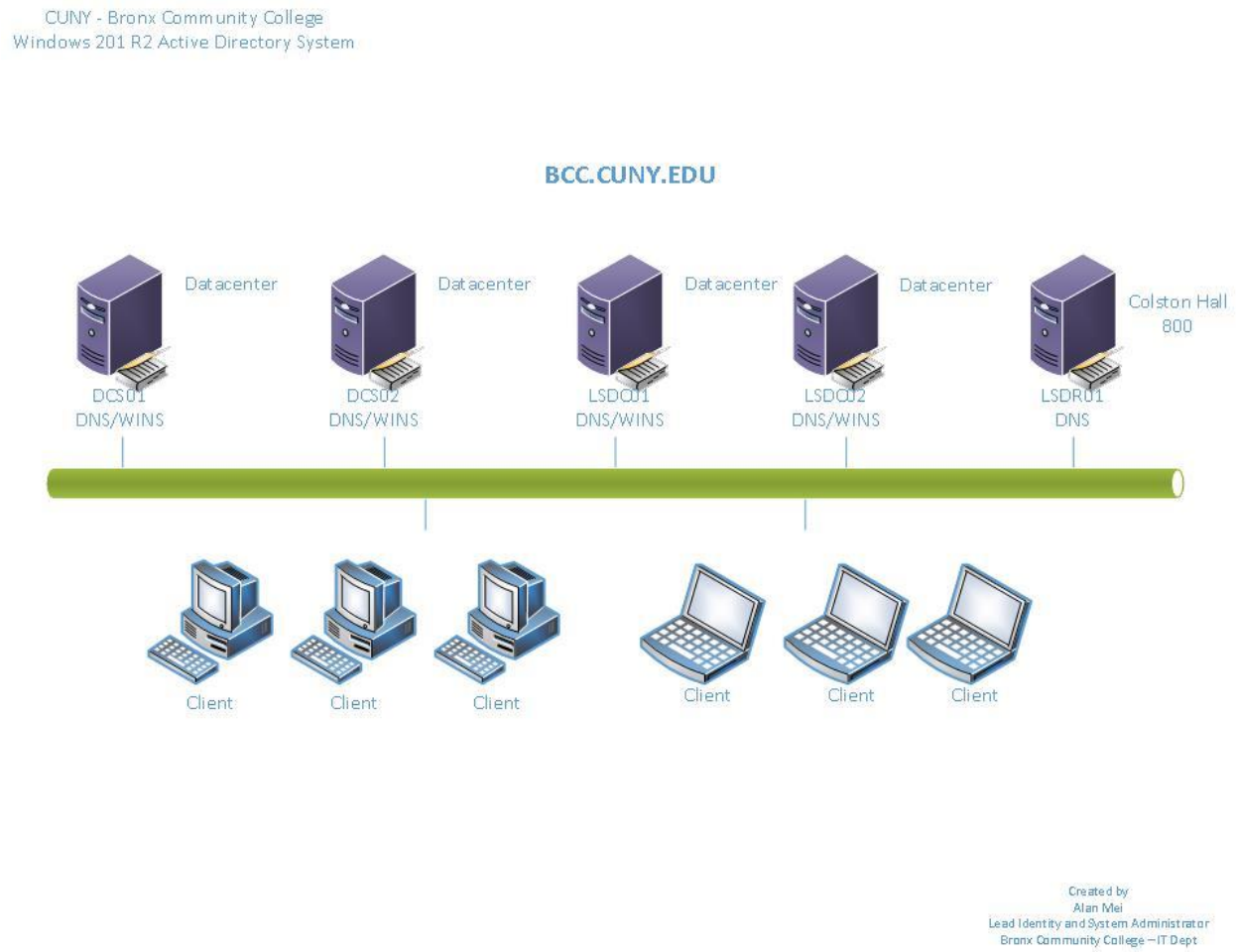
Instdev01	Monday	Tuesday to Friday
Lib01	Monday	Tuesday to Friday
Libqs01	Monday	Tuesday to Friday
mms02	Monday	Tuesday to Friday
Pps01	Monday	Tuesday to Friday
Ra	Monday	Tuesday to Friday
Sis01	Monday	Tuesday to Friday
Wa01	Monday	Tuesday to Friday

APPENDIX C

ACTIVE DIRECTORY DISASTER RECOVERY PLAN

Current Active Directory for BCC has five active domain controllers (DC). DCS01 and DCS02 are virtual. Eventually LSDC01 and LSDC02 will be removed, leaving only three active domain controllers running. In an event of any DC failure the other two will contain and replicate data across. If all domain controllers go down, we have a backup of the system state with backup exec to recover the entire domain in DRS01. DNS is installed on all Domain Controllers and replicate across all servers. Refer to Appendix B for backup details.

Active Directory Diagram

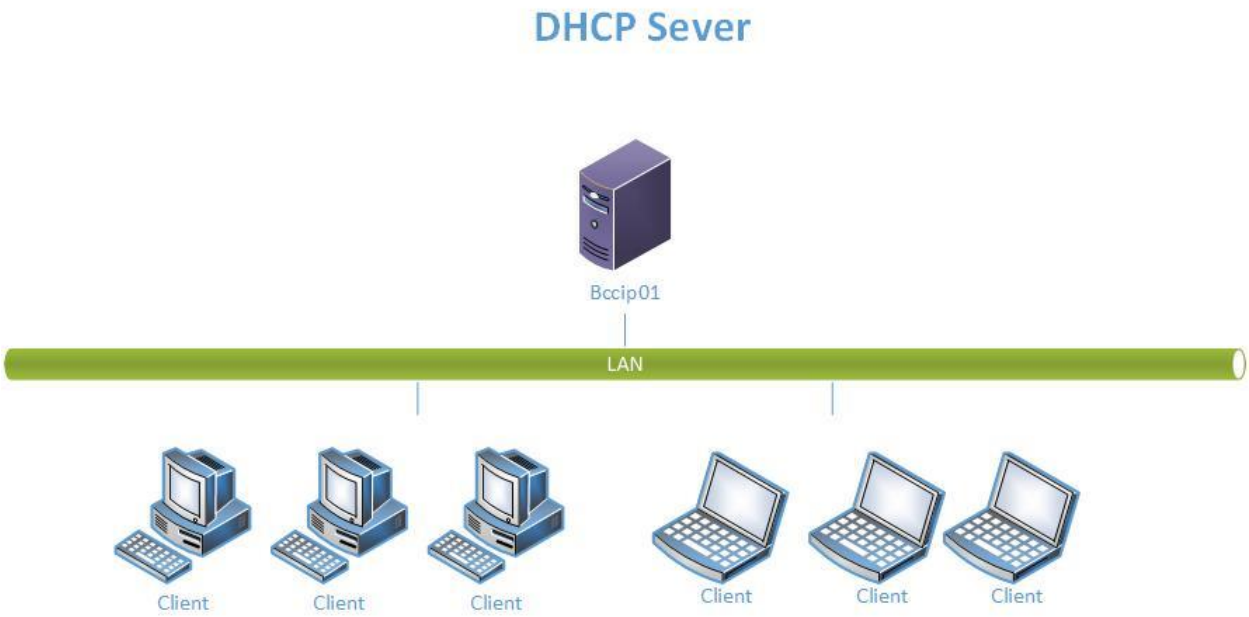


APPENDIX D

DHCP DISASTER RECOVERY PLAN

DHCP is a single server containing multiple scopes configuration. A configuration backup is stored in DRS01. In case of failure and we need to rebuild, a new installation of Windows Server will be required. Once the Operating System is configured, DHCP can be easily restored from a backup configuration. See Appendix B for backup details.

DHCP Diagram

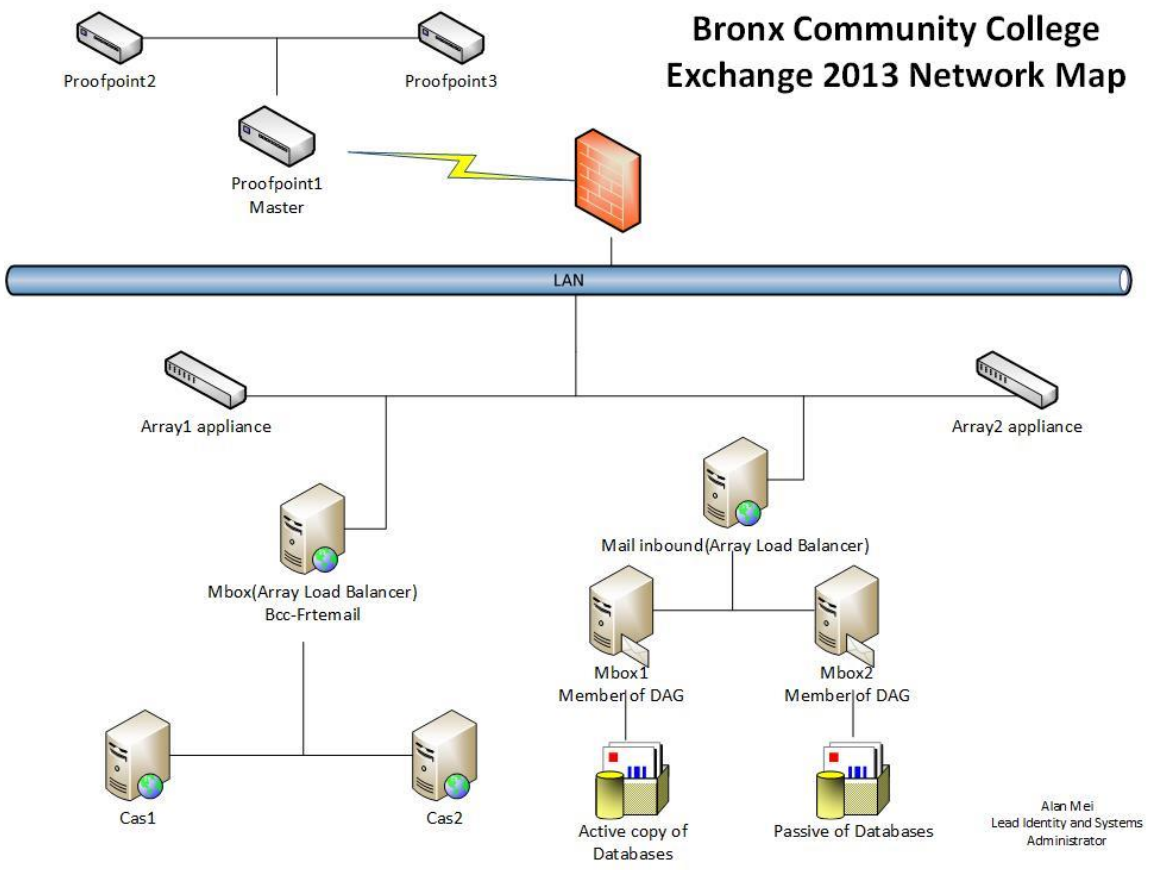


APPENDIX E

EMAIL DISASTER RECOVERY PLAN

Email is backed up from Monday to Friday with backup exec 2014. In case one of the databases goes down, databases can be restored from backup. Email databases are running with an active and passive copy to provide redundancy and to ensure business continuity. Refer to Appendix B for backup details.

Email Diagram



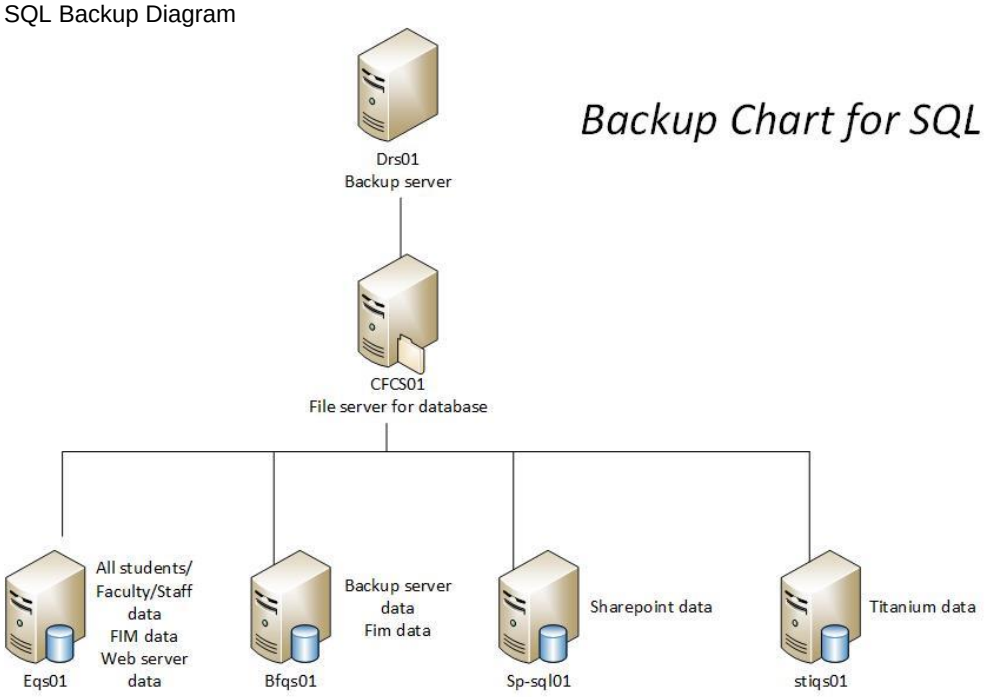
APPENDIX F

SQL DATABASES DISASTER RECOVERY PLAN

All SQL databases are backed up with a script to a file share server (cfcs01), and then all the databases are backup up from cfcs01 to drs01 with backup exec. If SQL failed, a new server will be rebuilt and databases will be reloaded from backup. SQL servers consist of the following: EQS01 | Bfqs01| Sp-sql01 | Stiqs01

Refer to Appendix B for backup details

SQL Backup Diagram

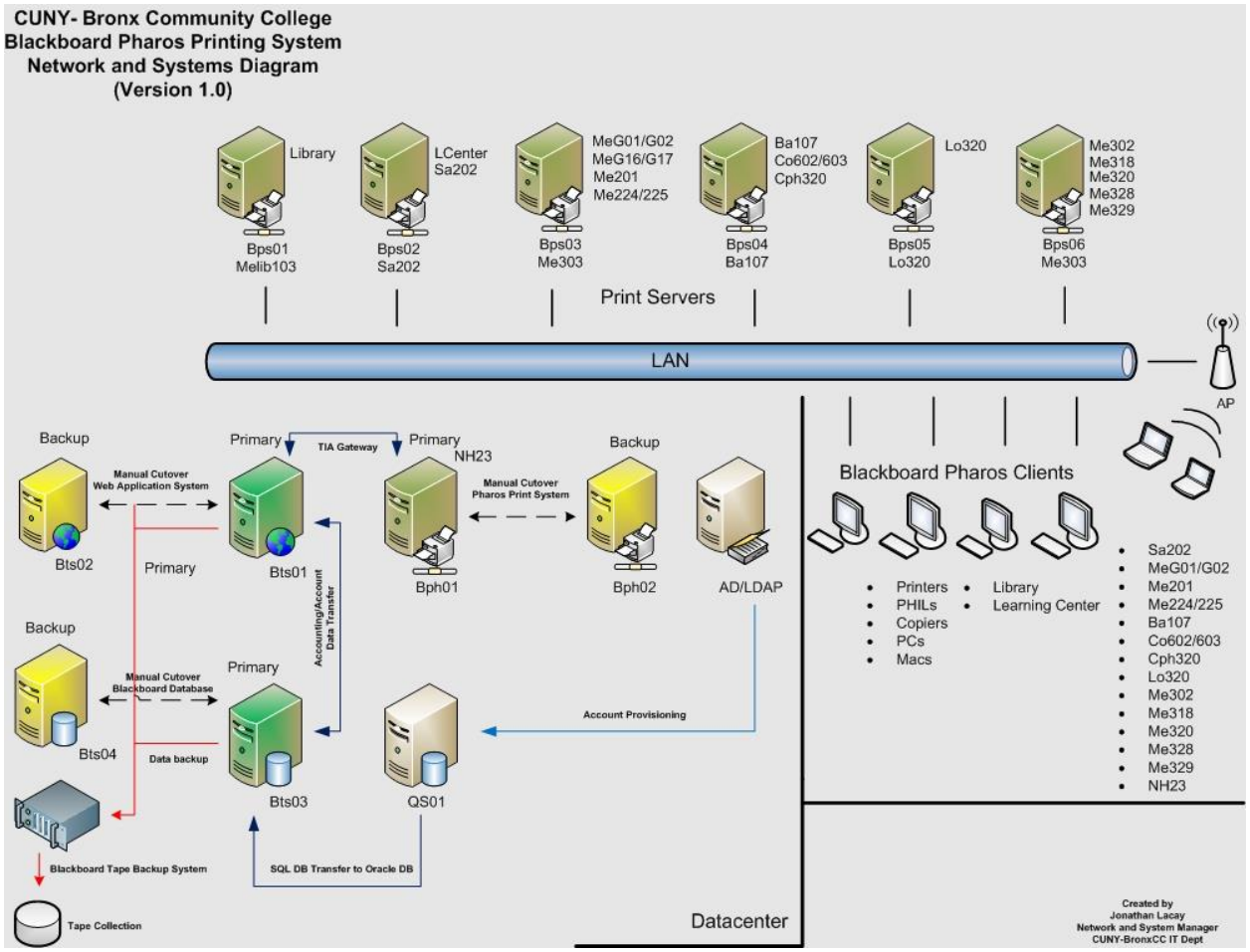


APPENDIX G

PHAROS AND BLACKBOARD TRANSACTION DISASTER RECOVERY PLAN

Pharos system has images backed up on DRS01. If any of the pharos servers go down we can rebuild the machine with the image and sync data across the system. If BTS01 or BTS03 need to be rebuilt, we have to contact Blackboard support and ask them to reinstall the application and import back databases. BTS03 runs Oracle and holds all databases information passing down to pharos. Databases are backed up daily on local server and then backup from Monday to Friday on DRS01 with backup exec. Refer to Appendix B for backup details.

Pharos and Blackboard Transaction Diagram

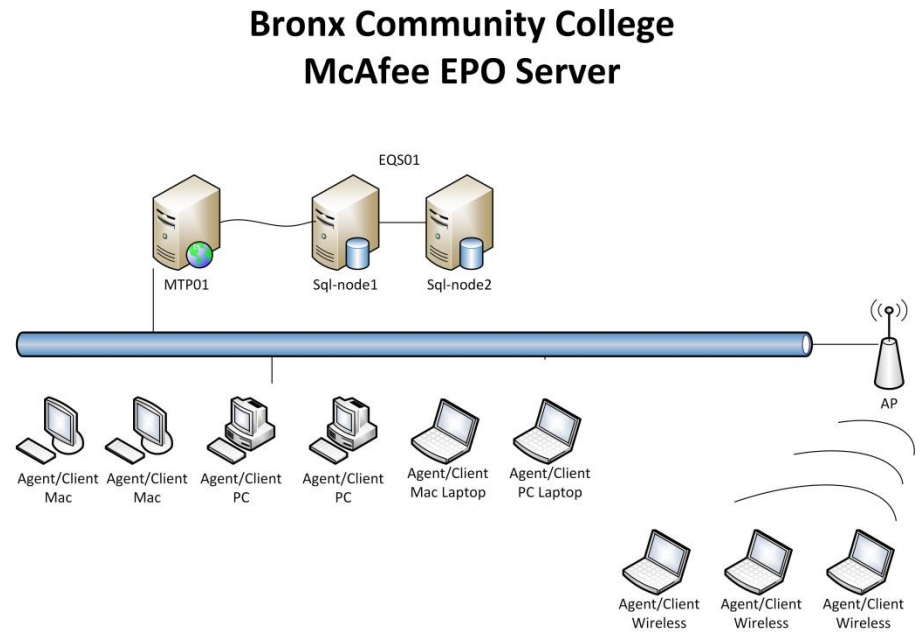


APPENDIX H

MCAFEE EPO DISASTER RECOVERY PLAN

McAfee EPO is a single server hosting all McAfee products. Database is connected to the eqs01 server. If server going down, we have to rebuild and reinstall EPO and connect it back to the database in eqs01. Refer to Appendix B for backup details

McAfee Diagram



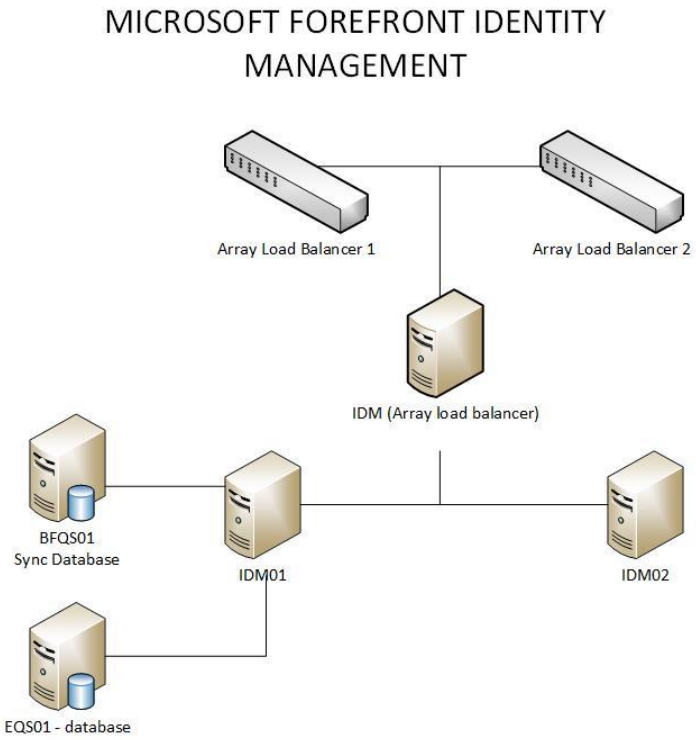
Alan Mei
Lead Identity and Systems Administrator

APPENDIX I

MICROSOFT FOREFRONT IDENTITY MANAGEMENT DISASTER RECOVERY PLAN

FIM is setup with 2 servers running with redundancy. If one server goes down we have to point all the services to the other server. If both servers go down, we have an image of the server in drs01. Restore image and reconnect to the database in bfqs01. Refer to Appendix B for more details.

Forefront Identity Management Diagram



See below on documentation on moving services to secondary server:

Restoring service to another machine
Log on with an account that is both a member of the FIMSyncAdmins group and sysadmin on the SQL Server.
Make sure the FIMSynchronizationService service is stopped on the machine that is "down". Run the following to determine the status of services:

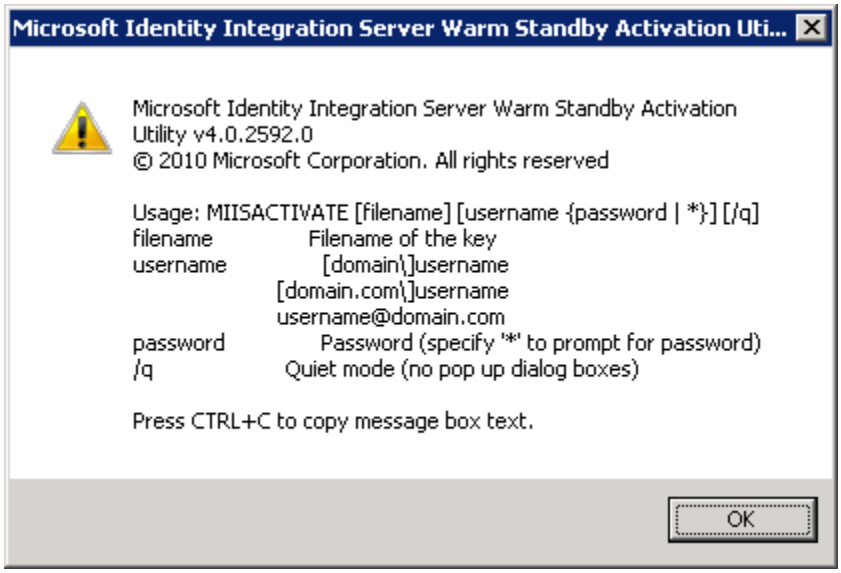
sc \\idm01 query FIMSynchronizationService
sc \\idm02 query FIMSynchronizationService

On the machine to activate, Run
"C:\Program Files\Microsoft Forefront Identity Manager\2010\Synchronization Service\Bin\miisactivate.exe" C:\FIM\FIM20110525.bin bronxcc\fimsync *
Where

Usage: MIISACTIVATE [filename] [username {password | *}] [/q]

filename	Filename of the most recent key (in this case it is FIM20110525.bin
username	[domain\]username or [domain.com\]username or username@domain.com
password	Password (or specify '*' to prompt for password)
/q	Quiet mode (no pop up dialog boxes)

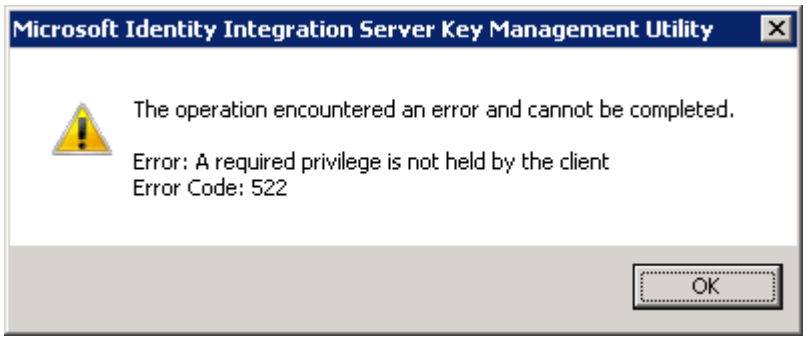
This is a copy of the popup that appears when running miisactivate.exe with incorrect parameters or without any parameters



The backup of the keys are in theC:\FIM\ folder. When news keys are generated, it is important that the new keys are copied to the FIM folder on IDM01 and IDM02.
A sample reminder when running miisactivate.exe in interactive mode.

You must enter the password for the FIMSync account.

If you fail after this step with the error shown below, the account under which you are running the MIISActivate.exe command does not have sysadmin privileges on the SQL database on sp-sql01.bcc.cuny.edu.



The account running MIISActivate needs to be sysadmin on SQL Server in order to change the credentials.

Command to create a new set of database keys. New keys should be generated whenever changes are made ot the database. It is critical that the new key is in the C:\FIM folder on both IDM01 and IDM02 or restore may fail.

miiskmu /e a:keyback.bin /u miisadmin *

Table 1 Parameters for the Miiskmu Command

Parameter	Description
/e	Exports the key set to a file.
a:*keyback.bin*	For the a: drive, specifies the file name in which you are saving the encryption key.
/u	Specifies the MIIS 2003 service account credentials.
miisadmin	Specifies the MIIS service account.

REM This is by wizard only without proper parameters
REM This will create a new sets of keys for the database.
REM "C:\Program Files\Microsoft Forefront Identity Manager\2010\Synchronization Service\Bin\miiskmu.exe" /e C:\FIM\FIM05252011.bin /u:miisadmin *