Chabot – Las Positas
Community College District

Information Technology Services

Disaster Recovery Plan

(General Version)

Note: Selected charts and tables are blanked out for security purposes

August 1, 2014

Submitted By
J. Methe
Chief Technology Officer

I. Table of Contents

This page intentionally left blank

II. Introduction

This document provides the Disaster Recovery (DR) and Business Continuity Plan for the Chabot-Las Positas Community College District (CLPCCD), including Chabot College located in Hayward, Las Positas College in Livermore, and the District Office in Dublin. The primary District Data Center that provides district-wide Enterprise systems to all locations is located in the Information Technology (IT) Building 1900 on the Las Positas campus.

The information presented in this plan documents the objectives, scope, offices of responsibility, system descriptions, and most importantly, the disaster recovery/emergency activation, execution, and reconstitution procedures.

The mission of the Chabot-Las Positas Community College District is to provide the leadership and resources to ensure that all students within the District will continue to have an equal opportunity to pursue and achieve their educational goals. With this in mind, Information Technology Services (ITS) plays a vital role in providing the computing resources to enable and enhance the students' learning experience. Increasingly, students rely on ITS systems to register for classes, conduct online instruction, use electronic mail to communicate with faculty, partake in multimedia and video-on-demand, research information using the Internet, and engage in a myriad of other applications. By the same token, District employees (staff and faculty), depend on ITS for day-to-day administrative tasks to support students and the colleges.

Clearly, CLPCCD is highly dependent on Information Technology resources such as telecommunications and network connectivity, computer systems, and applications, to fulfill its mission of high quality student education resources available 7x24x365. To meet this goal, the CLPCCD ITS enterprise, encompassing facilities and infrastructure, connectivity, computer systems, operating systems, and applications, must be reliable, resilient, and available to support computing services for students, employees, and the community. The primary purpose of the CLPCCD's Data Center and its Disaster Recovery plan is to ensure maximum availability of all critical systems and services.

It should be noted that this document includes sensitive information with detailed descriptions of hardware and software computer systems. This information is confidential to the Information Technology Services staff within the district. Given the level of detail that is presented, this information, if used improperly, could place CLPCCD in a vulnerable position with respect to viruses and other threats that would impact the IT infrastructure. As such, this document will be circulated to a limited set of District ITS and LPC IT staff, and is considered "For ITS Limited Distribution only" to those individuals who have a need to know this information in performance of their daily jobs.

III. PURPOSE

The primary objective of the CLPCCD Disaster Recovery plan is to protect and safeguard the District's Information Technology resources, including the network infrastructure, servers, applications, and data, and to ensure the ability to function effectively and ensure business continuity in the event of a disruption to normal operating procedures. This Disaster Recovery plan documents methods for response, recovery, resumption, restoration, and return after severe disruption.

The purpose of a Disaster Recovery plan is to formulate a strategy, define processes and procedures, and set in motion an action plan to effectively continue business and a return to normalcy after a disaster has struck. Specifically, the objectives are:

- Protect and safeguard the District's Information Technology resources, including the network infrastructure, servers, applications, and data.
- Ensure the ability to function effectively and ensure business continuity in the event of a severe disruption to normal operating procedures.
- Document methods for response, recovery, resumption, restoration, and return after severe disruption.
- Minimize the effects of a disaster on day-to-day operations.
- Present an orderly course of action for restoring critical computing capabilities.
- Describe an organizational structure for carrying out the plan.
- Provide information on personnel and staff and who will be responsible for carrying out the plan.
- Identify and describe the infrastructure, equipment, computer hardware, and applications.
- Identify and classify the threats and risks that may lead to a disaster.
- Define the resources and processes that need to be in place to recover from a disaster.
- Define the reconstitution mechanism to get business back to normal from a disaster recovery state.

District ITS has established district standards and best practices for ensuring hardware and software redundancy of the critical district services. District standards are designed to minimize system interruptions and to reduce the system recovery time when failures occur. Backup systems are available for the primary District Data Center operations and environment. Hardware redundancy is in place for all the critical application servers. Application redundancy is achieved where feasible, based on vendor licensing allowances. In each of the applicable sections, the backup and redundancy capabilities are explained in detail for those specific computing resources.

For the predictable failures, which include computer equipment failure, power failure, communication line failure, or damaged computer files, the following procedures will be invoked:

1. The responsible individual will determine the nature of the equipment failure and take appropriate action to coordinate repair and restoration of services, or
2. in the event that the responsible individuals are unavailable, ITS management will delegate responsibility to the appropriate alternate staff.

For the exceptional failures, the following general strategies would be used:

1. If any portion or all of the facilities supporting the District's central computing resources were damaged beyond use, ITS management and other District management would work with the District's insurance carriers to determine whether to pursue repair or to secure temporary facilities.
2. If the damage is to be remedied by repairs, ITS management will direct the process in compliance with established District procedures.
3. If temporary facilities are required, appropriate contracts will be let to provide for rental facilities and equipment as needed. For the IBM System supporting Banner, a mutual assistance agreement with San Mateo Community College District has been established to provide temporary services for critical Banner applications as identified based on the severity of the outage. Refer to Appendix A.

IV. SCOPE

The Disaster Recovery plan described in this document pertains to Information Technology resources hosted at Chabot College, Las Positas College and the Dublin District Office.

These resources are as follows:

- Network infrastructure includes the telecommunication circuits, firewall devices, routers, switches, and cabling.
- Servers hosting the applications and storing data used by District employees. These servers include the Banner System, other third party applications that interface with the Banner System, e-mail, Internet, Intranet, file sharing, network authentication, DNS, DHCP, and network management.
- Data stored either in the servers or on storage area networks (SANS), including documents (Word, Excel, PowerPoint), e-mail correspondences and attachments, system-related files, web content, and application programs.

The Disaster Recovery plan is designed to address two levels of service interruption:

- Predictable failures confined to specific systems or functional areas such as electrical power failures, computer or network equipment failures, HVAC failures, communications line failures, or file damage.
- Exceptional failures with broad scope of impact on computer services produced by events such as a computer data center related fire, flood, earthquake, etc. where the event does not cripple District operations as a whole.

The Disaster Recovery plan is not designed to address conditions of widespread damage throughout the District. However, it will help define the activities that might be required to restore central computing services to the District in the event of broad catastrophe.

An important component of a disaster recovery plan is to identify the threats and risks that can bring about disasters that can severely impact business continuity. A disaster recovery plan employs measures to prevent or mitigate the effects of a disaster beforehand and minimizes the risks. Some of the higher risks threats are identified here that could be natural and human-created.

- Earthquake: The threat of an earthquake in the San Francisco Bay Area is high, and therefore ranks as the most likely cause of a disaster. Scientists have predicted that a large earthquake along the numerous fault lines may happen any time in the next few years. An earthquake has the potential for being the most disruptive for this disaster recovery plan. There is also a likelihood of fire occurring after an earthquake due to gas leaks. If the campus buildings and data center and network infrastructures are heavily damaged, restoration of computing and networking facilities following a bad earthquake could be very difficult and require an extended period of time due to the need to do wide-scale building repairs, and dependencies on service providers to repair their infrastructure. .

- Fire: The threat of fire on the campuses, especially in the District's ITS Data Center area located on the Las Positas campus, is very real and poses the highest risk factor of all the causes of disaster mentioned here. The Data Center building 1900 is filled with electrical devices and connections that could overheat or short out and cause a fire. During hot summers, the treat of brush fire from the surrounding areas is also real. Also, fire can be human created; e.g., arson.
- Computer Crime: This is becoming more of a threat as systems become more complex and access is more highly distributed. With the new networking technologies, more potential for improper access is present than ever before. Computer crime usually does not affect hardware in a destructive manner. It may be more insidious, and may often come from an unexpected external source or from within. Viruses and worms can be imported from the outside causing denial of service to critical systems.

V. DISASTER RECOVERY MANAGEMENT AND TECHNICAL TEAM

The following management and technical teams are responsible for supporting the CLPCCD Disaster Recovery (DR) plan and will contribute as necessary based on their core competencies:

- Chief Technology Officer (CTO): Primary point of contact for the Disaster Recovery plan. Manages and coordinates all IT resources and provides technical expertise, standards, policies, and procedures to ensure restoration of services in the event of a disaster.
- Information Technology Services (ITS), Chabot College Computer Services and LPC Technology Staff: Provides the technical skills to salvage the critical systems and services from hardware and software malfunction, to preserve the integrity of the systems data, to coordinate with vendors as needed during the disaster, and to restore the Data Center and College Server services as soon as possible in accordance with the priorities established by the DR plan.
- Maintenance and Operations: Provides day-to-day maintenance and monitoring of IT infrastructure to ensure viability of HVAC, Fire Alarm/Suppression, electrical, and plumbing systems in support of the DR plan. Coordinates all services for the restoration of support infrastructure.
- Purchasing and Business Services: Manages and coordinates the purchasing of hardware and software in support of the DR plan.

Refer to Section VIII for “ITS Emergency Contact Information” and for “M&O Emergency Contact Information” for both Chabot and Las Positas Colleges.

Refer to Section XII “Initiation of the Disaster Recovery Plan” for the various scenarios with action plans for responsible parties.

VI. IT INFRASTRUCTURE

CLPCCD ITS infrastructure that houses computer systems, telecommunications, and data networking equipment is located at LPC building 1900, LPC building 1900A, Chabot building 200, Chabot building 300 and the District office in Dublin. Each of the primary facilities is discussed in more detail below.

ITS ADMINISTRATIVE DATA CENTER AND LPC INSTRUCTIONAL SERVER ROOM, LPC IT BUILDING 1900

The nerve center of CLPCCD's ITS infrastructure is located in Las Positas College (LPC), building 1900 IT Building. The facility houses the IBM Enterprise servers that host Ellucian's Banner System, which is the District's ERP application. The data center also contains HP stand-alone and blade servers and SAN infrastructure that host critical applications: Banner auxiliary applications such as Luminis, Degree Works, LPC electronic mail and user data, Intranet and Internet web services, and network management tools.

The LPC Instructional Server Room contains servers used in support of LPC instructional requirements. These are stand-alone HP servers running applications such as DNS, DHCP, Application, Web, SARS, AMAG Security, imaging, file and print services,

As part of the construction of the LPC IT building, a number of sophisticated systems were designed to provide a robust operating environment. They are HVAC control, Humidity, Power, and Control and Monitoring systems. Each of these systems is described below.

HVAC Control

The Heating, Ventilating and Air Conditions systems for the network and server rooms in the IT building consist of the following:

- ❖ **Primary Air Handler Unit (AHU-2A):** This supplies the heating/cooling for the Administrative computer room, Network room and LPC Server rooms. This unit is fed from the Central Utility Plant (CUP).
- ❖ **Secondary Air Handler Units (AHU-2B):** This unit is a redundant unit that also supplies heating/cooling for the Administrative computer room, Network room and LPC Server rooms. This unit is fed from the Central Utility Plant (CUP). This unit is activated if a failure of the Primary AHU-2A occurs.

- **Supplemental 5 Ton System:** In addition to the Primary and Secondary AHU systems, a ceiling mounted HVAC system is installed in the Administrative Computer room. In the event of a temperature rise in the computer room, this unit is triggered into operation at an elevated temperature of 78 degrees. This provides additional cooling directed towards the IBM Enterprise Server air intake vents.

The water source for the HVAC systems comes from the Central Utility Plant (CUP). The CUP is equipped with a primary and secondary pump/chiller. The primary pump/chiller operates during the day to deliver cold water from ice storage to the IT Building systems and the rest of the LPC campus on the CUP loop. This primary system operates from 6am to 10pm. At 10pm, the secondary pump/chiller comes in to operation while the rest of the CUP is in ice-making mode. In the event of a failure of the primary pump/chiller, the secondary pump/chiller initiates into service. During ice-making mode, the primary pump/chiller initiates back into service if the secondary pump/chiller fails.

If both these CUP systems fail, the IT Building is equipped with a backup chiller. The backup chiller automatically initiates into service to feed the AHU2A/2B. Typically, this would occur in the following scenarios:

- CUP chillers, primary ***and*** secondary, fail
- Power failure on campus which takes down the CUP equipment
- EMS panel in the IT building loses connectivity to the main monitoring system.

Except for planned power outage needed for maintenance and/or construction, it is not expected that the Backup Chiller would run regularly. Monthly testing is scheduled to insure correct operation. A fail-safe mechanism has been recently designed that enables the manual activation of the Backup Chiller in the event of a catastrophic CUP failure. This allows further protection of the Data Center server and network equipment so as to minimize the chance of overheating for this critical infrastructure.

Humidity Control

Each of the Network and Computer rooms are equipped with a Humidifying system which senses and releases moisture to maintain the proper humidity range.

Power for Building IT Building Server and Network Rooms

CLPCCD District ITS disaster recovery posture is reliant on power continuity through UPS protection and generator. This provides a basic operating environment in the event of power failure.

The IBM Enterprise servers in the data center are connected to a large UPS system. If electricity is lost, the UPS powers the computer room. The UPS is network attached and has the ability to send SNMP messages.

The data center is equipped with new Eaton Powerware UPS systems for power-protection. The systems deployed are as follows:

- **Powerware 9355 UPS –** This UPS is a dedicated UPS to provide service to the IBM Enterprise Servers supporting the Banner System, which is located in the Administrative Computer Room. It connects to the electrical panel UR1, which serves the electrical circuits to the IBM Enterprise servers. This UPS is sized to support a 40 minute uptime, which is the time it takes for the execution of a script to do a clean shutdown of the IBM Servers.
- **Powerware 9395 UPS –**This UPS provides service to the LPC Server Room, Network room, and the remaining Administrative Computer Systems. It connects to the electrical panels UR1-4, which serve the electrical circuits to the rooms just listed, and a select number of power outlets in certain offices in the IT building.

These UPS systems are all powered by a 400KVA Backup Generator. The Generator is housed in the fenced lot immediately beside the IT building. A 400 gallon fuel tank feeds the generator. In the event of a power failure, an automatic transfer switch (ATS) initiates the generator to start. The generator is fully running to supply power to the UPS systems in less than 60 seconds. The fuel tank is sized to provide 12 hours of runtime for the fully deployed Network and Computer rooms. CLPCCD M&O maintains an open PO with a refueling company who will come onsite to refuel the tank on a scheduled or emergency basis. The generator is tested monthly to insure correct functionality.

Control and Monitoring

There are several levels of control and monitoring:

- **UPS Control and Monitoring –** The UPS systems are equipped with SNMP network cards to provide web access for monitoring. They are also equipped with temperature probes to measure the temperature in the B1900A, and the Administrative Computer room (two locations). In the event of a power or temperature issue, the UPSes have been configured to email a distribution list with the details of the issue. The UPS trigger for high temperature alerts is currently set for 25C (~77 degrees F).
- **Security Monitoring -** The AMAG security system monitors temperature probes in the Network and Computer room using Enviro-Alert stations. In the event of a high temperature situation (currently set for 74 degrees F), the AMAG server triggers a visual and audible alarm to the monitoring staff. The monitoring staff then alerts with phone calls to address the high-temperature malfunction. A low temperature threshold of 55 degrees F is also configured.
- **Allerton Monitoring** - The Las Positas campus uses an Allerton system as the comprehensive monitoring system for building automation systems. This system receives alerts from the EMS panel, HVAC devices and status probes in the IT Building. Response to alerts of abnormal functionality trigger emails and telephone contact to for action.

Since many of these alerts are generated by equipment malfunctions, CLPCCD M&O is contacted as the first responders. CLPCCD District ITS is contacted secondarily to be ready in the event that the situation cannot be corrected, and the servers and equipment need to be shut down.

LPC BUILDING 1900A MPOE/MDF

The LPC Campus has a centralized network and telecommunications facility that houses the AT&T and CENIC telecommunication equipment, which is essential for wide area connectivity and the phone system communication. These facilities contain the campus telephone system, the cable plant and network equipment such as firewalls, routers, and switches that provide local area, wide area and Internet network connectivity for the campus. At LPC, the telecommunication facility is located in building 1900A, which is next to the IT Building. The following systems are installed.

HVAC Control

In Building 1900A, a series of new HVAC units are installed. This consists of a 10 Ton unit which directs airflow towards the telephone equipment in the MPOE end of the building. Two five (5) ton units provide airflow directed at the MDF end of the building. In the event of a failure of one of the units, the remaining units can continue to provide cooling to building, while repairs are initiated.

Building 1900A has been equipped with new Eaton Powerware UPS systems for power-protection. The UPS deployed is:

- ❖ **Powerware 9390 UPS –** This UPS provides service to the B1900A network electronics and HVAC systems. This UPS is sized to support a 10 minute uptime. This UPS is also connected to the generator that powers the LPC IT Building.

UPGRADED SERVER ROOM AT CHABOT COLLEGE

Building 300 modernization was completed in early 2012. The new Server room provides a robust environment for Chabot College servers and CLPCCD District Internet servers.

The construction modernization in Building 300 server and network rooms were improved in the following areas:

- ❖ Computer room layout – A more efficient computer room layout with six four-post cabinets provides: (1) more racking space for server equipment, (2) more circulation and access for maintenance, (3) defined hot aisle/cold aisle for efficient cooling control (4) increased network connectivity to Category 6A data cable (5) more available and accessible power. All server and equipment cabinets are seismically installed and rated for zone 4 disturbances.

- Updated network room – The network room (MDF) is equipped with new racking, cable management, more efficient fiber patch panel layout and Category 6A data cabling to station jacks. The Cisco core switch for the campus is mounted in the network rack in the MDF, and provides centralized routing to the entire campus. The CENIC router has also been moved to the MDF for improved uptime.
- New UPS – The current 30KVA UPS was replaced with a new UPS capable of supporting a 45KVA load. A transfer switch allows the transition to the building generator to supplement the UPS power, in the event of a facilities outage. The generator supports power to the Chabot Data Center, MDF, and related support systems that include HVAC, Inergen, Fire Alarm/Suppression, Security, etc.
- New HVAC - The HVAC systems has been replaced and is now integrated with the campus building monitoring system (Allerton).
-

The B300 server room contains standalone District servers for mail, DNS and Internet access. Chabot College servers for file/print services, SARS, AMAG, Library, Web, Tightrope, and instructional applications are also housed in this server room.

CHABOT COLLEGE BUILDING 200 MPOE

The telecommunications facility housing AT&T and CENIC equipment that provides Internet and WAN connectivity for Chabot College is located in Chabot building 200. AT&T provides UPS backup battery supply for their fiber termination cabinet in case of power outage.

Campus telephone and voicemail systems are centralized in the B200 MPOE. The campus telephone system is upgraded to a state-of-the-art Avaya system with AVST voicemail. Housed in B200, it is supported by a 30KVA UPS, repurposed from B300 when the construction project upgraded the B300 UPS, as described above. The 30KVA UPS will sustain power to the telephone system for several hours, allowing dial tone to work throughout the campus during an emergency or scheduled power outage.

All network equipment and servers in B200 are mounted on racks that have been installed to meet California state earthquake seismic requirements. The racks are bolted to the concrete and are secured at the top to 12” wide ladder racking that are connected to each side wall. The network equipment is also powered by the 30KVA UPS for sustained uptime during power outages.

If required, a portable generator can be wired into the electrical panels of B200, for sustained power during extended and planned outages.

DUBLIN SERVER/IDF ROOMS

At the District office location in Dublin, the third floor houses a server room which contains servers for print, mail and file services and backup. These servers are connected on discrete UPSes to allow up to 30 minutes of uptime, thereby facilitating a clean shutdown of the applications before the UPS batteries drain. The UPSes also provide power protection for the key network devices in IDFs on the first and third floors.

VII. NETWORK INFRASTRUCTURE

CLPCCD operates three types of networks that provide connectivity: Local Area Network (LAN), Metropolitan Area Network (MAN), and Wide Area Network (WAN). Each type of network is described below.

CAMPUS LAN (LOCAL AREA NETWORK)

Chabot and LPC campus LANs are comprised of Cisco routing and switching products to serve as the respective core campus network topologies. This offers best-in-class capability and exceptional manufacturer's support. The standardization of command access for configuration and maintenance allows for consistency of operation.

The campus LANs have undergone a total equipment reconfiguration and upgrade in the past couple of years. Key tenets of this new network architecture are as follows:

- ❖ High Availability: Incorporate as much redundancy and diversity into the design that is cost effective in order to ensure maximum uptime and permit software and hardware maintenance to be performed without downtime. To accomplish high availability and redundancy, each campus has two Cisco C catalyst 6509 router/switches with and intelligent engine modules and redundant power supplies.
- ❖ Security: Network segmentation into multiple security zones to isolate user communities from each other and to protect key areas of the network from worms and viruses. This segmentation is accomplished through virtual local area networks (VLANs), Access Control Lists (ACLs), and firewalls on a per building and usage basis.
- ❖ Upgraded Fiber Backbone Building Connectivity: As building construction has provided, an upgrade of the fiber backbones to allow for high bandwidth, diverse connectivity is a basis for the building connectivity design.
- ❖ Redundant Server Connectivity: Wherever possible, redundant, high-performance connections to mission-critical servers by using dual network interface cards have been installed to limit downtime caused by NIC card failures.
- ❖ Extensive support of advanced switching features: Advanced features such as Quality of Service (QoS) and security parameters are important design requirements to support high-quality video conferencing, responsive administrative and educational application access, and reduce the impact of worms and viruses.
- ❖ Manageability: The new architecture is built upon consistent hardware platforms and software configurations. Native IP, an Internet standard, is the standard routing protocol. All network devices are SNMP-managed from a centralized network management server, where alerts for outages or unusual network activity are transmitted through email or texting to CLPCCD ITS support staff.

To achieve a highly available and redundant LAN architecture, the campus' core network backbone consists of Cisco Catalyst 6509 switches with 10Gbps and 1Gbps fiber links, 10/100/1000 switching ports, and redundant power supplies. Additionally, in large campus buildings that are densely populated with computers, Cisco 4506 switches with redundant power supplies are installed. The smaller and less densely populated buildings are equipped with Cisco 3560 switches.

At the Chabot Campus, the switches are connected to new or renovated buildings using single mode fiber with 1000Base-LX connectivity, and multimode fiber with 1000Base-LX connectivity over mode-conditioning cables to legacy buildings. Limited 1000Base-SX and 1000Base-LX riser connections have been implemented in buildings that are equipped with multiple telecommunications closets. If cabling and hardware is available, buildings with multiple IDF closets and switches are connected with discrete uplinks to the MDF core switches to improve survivability in the event of equipment failure.

At the Las Positas Campus, the switches are connected using the existing single mode fiber with 1000Base-LX connectivity. Limited 1000Base-SX and 1000Base-LX riser connections have been implemented in buildings that are equipped with multiple telecommunications closets. If cabling and hardware is available, buildings with multiple IDF closets and switches are connected with discrete uplinks to the MDF core switches to improve survivability in the event of equipment failure.

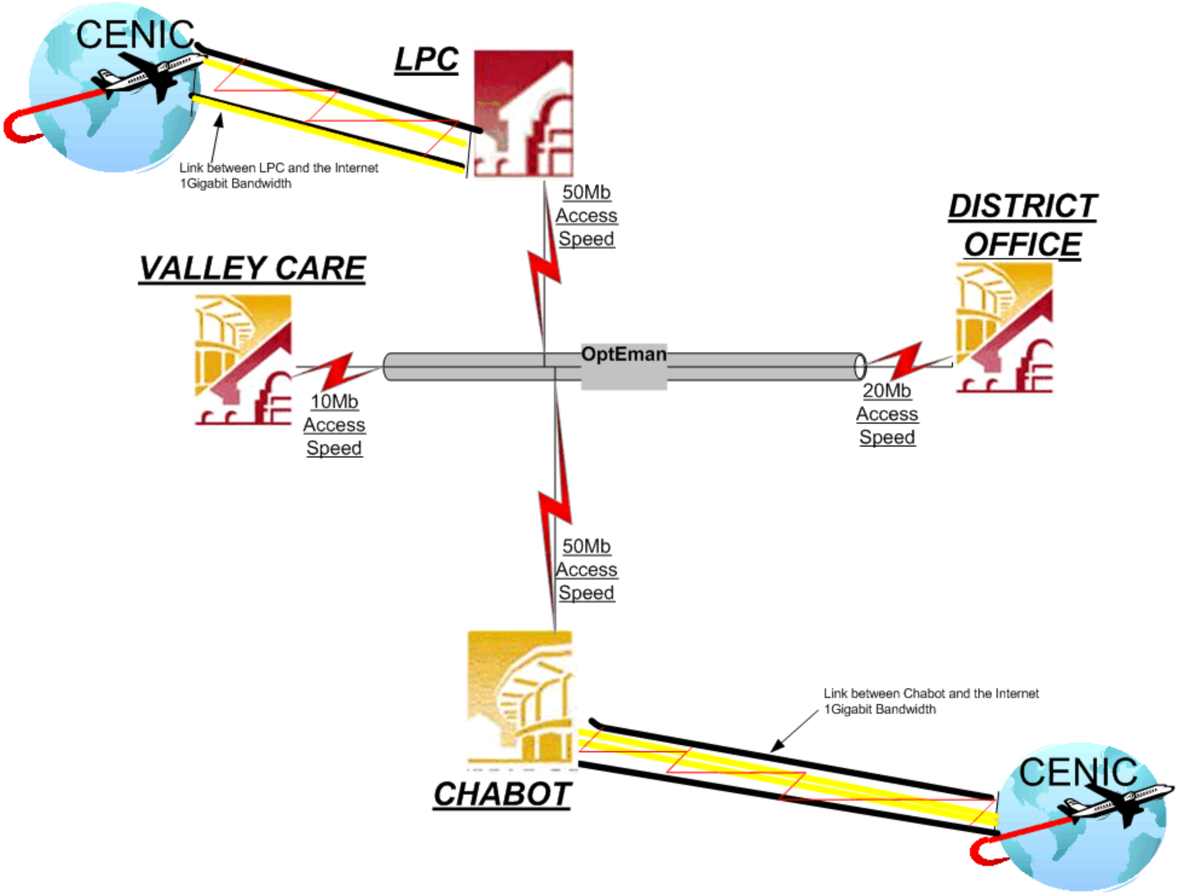
For the core campus LAN routers and switches, Cisco SMARTNET maintenance agreements have been purchased to provide 7x24x365, four-hour response time to replace failed hardware components. High density 4506 switches are supported with 8x5xNBD Cisco SMARTNET contracts. For the smaller building 3560 switches, ample spare parts are available and ready to be deployed as necessary.

OPT-E-MAN NETWORK (FOR INTERNET OUTAGE RECOVERY)

As part of Bond Measure B, the District upgraded all connections between all of the CLPCCD sites. In September 2008, the District implemented the AT&T OPT-E-MAN network, based on Ethernet over fiber. Metro Ethernet is a robust technology that utilizes carrier fiber optics to achieve high speed network connectivity between remote locations. Ethernet is an industry-accepted, proven local area network (LAN) technology that is used to connect PCs to servers located in a building. Recently, Ethernet LAN has been expanded to provide network connectivity for remote sites, hence the term metropolitan. Metro Ethernet takes advantage of high speed connections to servers located remotely. Metro Ethernet is expandable. If the need arises for additional bandwidth in the future, bandwidth can be increased transparently without disruption to the existing environment.

CLPCCD's Opt-E-Man was upgraded January 2014 to increase the bandwidth to 20 megabit/second from the District office to the college campuses and 50 megabit/second between college campuses. An additional 10 megabit/second Opt-E-Man connection was provided at Valley Care Hospital to support the Chabot Nursing curriculum. This topology not only provides necessary bandwidth for day-to-day CLPCCD activities, but also the option to re-route traffic if needed during a network failure.

Below is an illustration of the CLPCCD Network:



WIDE AREA NETWORK (WAN)

Internet connectivity and student and employee access to resources via the Internet is crucial to student learning. With the Internet, the colleges have the most up-to-date technology to enrich, enhance, and broaden students' learning environments through applications such as online courses, video-on-demand, video conferencing, collaborative learning, and rich multimedia experiences.

In partnership with our service provider, CENIC and through the State Chancellor's office and AT&T, one gigabit of network connectivity for each college has been provisioned. Moreover, CENIC has provisioned for redundant and alternative fiber paths and protocol routing within the Internet cloud to mitigate major fiber disruptions.

FIREWALLS

To provide Internet connectivity for the campuses, and more importantly secure the internal networks, Cisco ASA 5520 firewalls were installed in 2011(to replace the PIX 515E firewalls). Each campus has a pair of ASA 5520 firewalls, equipped with unlimited licenses, multiple Ethernet interfaces and VPN accelerator cards. The ASA firewalls are running in master-slave failover mode, so that if the master ASA fails, the slave ASA converts to the master and takes over network transactions automatically.

At the Chabot campus, the ASA 5520 pair provides connectivity to the CENIC gigabit link, the internal networks, and the administrative and instructional server DMZ networks. At the LPC campus, the ASA 5520 pair provides connectivity to the CENIC Internet gigabit link, the internal networks and the instructional server DMZ networks.

The Cisco ASA firewalls have Cisco SMARTNET maintenance support at 7x24x365, 4-hour response time. Further, Virtual Private Network (VPN) has been configured for each campus ASA firewalls. VPN allows CLPCCD ITS network technicians to securely access the internal network during off-duty hours to monitor, manage, and troubleshoot the network.

SECURITY

The District ITS department is responsible for maintaining security and access to administrative servers at all sites, including the Banner application access. College Computer Services are responsible for security to the servers they support. Security includes network accessibility and physical security.

Access

At the District office, the servers and network equipment are located in locked rooms with card readers, only accessible to District ITS staff with the correct access programmed on their security card key. The AMAG security system logs access to the server/network rooms whenever a door is opened.

At Chabot campus, the network MDF and District ITS and Campus servers are located in locked areas in Chabot building 300. The college computer staff monitors access to these rooms. The area is protected with card key and keypad access, and monitored by the campus AMAG server

At LPC campus, core network equipment is located in building 1900A. Campus and District ITS Administrative servers are located in building 1900. Card key and pass codes are required for entry any time of the day. These facilities are alarmed after hours, and monitored by the campus AMAG server.

Overall network security is the responsibility of the District ITS department. Like the servers, the core network equipment is installed in locked areas with restricted access. Some of the edge equipment is more vulnerable because it is located in IDF spaces in classrooms and shared areas. As buildings are renovated and modernized, network equipment will be stored in locked IDFs with restricted, card key access. The CLPCCD ITS Network Cabling Standards have clearly documented the requirements for separate, secure Information Technology and Telecomm rooms. The Security Master Plan issued in the Fall of 2005 has identified Information Technology and Telecomm rooms as secure locations that require separate card-key access and is restricted to IT staff.

Passwords

District ITS department maintains three separate user accounts. This includes Novell Directory Services (eDirectory) accounts/Groupwise e-mail, Banner System, and IBM AIX user accounts. IBM-AIX passwords are case sensitive and users are required to change them frequently. Banner System and other application passwords are set to expire on a predefined schedule to require users to change their passwords as prompted by the application. Users are recommended to change their Novell and email passwords on a regular basis as needed.

At Chabot, Instructional Domain Authentication passwords are managed by the Chabot Computer Support staff. This includes faculty passwords in Microsoft Active Directory environment and Windows Local Accounts. There are no individual student user accounts currently in use at Chabot, instead generic student accounts, with limited access, are used by the students to access the Instructional Network resources.

At LPC, Instructional Domain Authentication passwords are managed by LPC Technology Support staff. This includes faculty passwords in Microsoft Active Directory environment and Windows Local Accounts. There are no individual student user accounts currently in use at Las Positas. Instead generic student accounts, with limited access, are used by the students to access the Instructional Network resources.

Network device passwords, such as routers and switches are also maintained by the District ITS department and changed as needed to secure access. Passwords are formatted with special characters to provide an additional level of security. Switches have a user level logon to allow Chabot and LPC computer support technicians to modify VLAN assignments as needed at each campus.

Anti-Virus

Virus and worm attack is possible on the network, particularly on the Instructional network. CLPCCD uses anti-virus protection on each desktop to limit the possibility of virus attack.

Symantec's Endpoint Protection version 12 is used on the District administrative workstations. The virus definitions are updated to the ITS-2K Windows server, and the administrative workstations automatically update from the current signature file directly from the server or some directly from Symantec.

At Chabot College, Symantec's Endpoint Protection version 12.1 is located on the APPSRV server. The virus definitions are updated from the Symantec web site and user desktops download the definition files from the local server daily.

At LPC, Symantec's Endpoint Protection is provided on specific servers. The virus definitions are updated from the Symantec web site.

IBM ENTERPRISE SERVERS (FOR BANNER SYSTEMS)

CLPCCD utilizes Ellucian's Banner as the core administrative, Enterprise Resource Planning (ERP) system. Banner supports applications for Student Services, Academic Services, Financial Aid, Finance, Human Resources, and Payroll functions within the district. Banner utilizes Oracle as the database engine.

Banner applications are as follows:

- Banner (Internet Native Banner INB) – Student, Financial Aid, Finance, HR, Payroll
- Class Web (web-based for Student)
- Luminis student portal
- Web for Finance (web-based)

- Web for Faculty (web-based)
- Web for Employee (web-based)
- Web for Financial Aid (web-based)
- Crystal Enterprise (WebI) for queries and reporting
- Degree Works
- College Net Room Scheduling

In the near future, CLPCCD will be adding Enrollment Management Suite, Document Management system, and ad hoc query/reporting tools, like Operational Data Store (ODS), Data Warehouse and Cognos.

As part of the data center move, two new IBM servers were purchased and installed. The first IBM server is installed in the ITS Administrative Computer room in the Las Positas IT Building. The second IBM server is colocated in the Administrative Computer room and functions as a redundant system. Hardware and software configurations are replicated so either server can operate as the primary Enterprise server. Vision Solutions software, Echo Cluster and Echo Stream provide full software replication for the operating systems. Oracle database and user data are stored on the primary server and duplicated on the second server. In the event of a failure of the server acting as primary, the other IBM server can be brought into service to serve as the primary server.

Besides the primary IBM Enterprise servers, the Banner System includes other supplemental servers for Self-Service CLASS-Web services and Internet Native Banner (INB) servers. Both the CLASS-Web and INB servers have hardware redundancy and application redundancy to be used as backup in the event of an unexpected failure. These backup servers can be swapped out as needed to fully restore these specific Banner services.

Below is a list of IBM systems and ancillary devices supporting SunGard Banner:

Product Type	Product Model	Product Serial Number	Description
1814	20A	78K0HRN	DS5020
1814	20A	78K0HR6	DS5020
1814	52A	78K0HR7	DS5020
1814	52A	78K0HR8	DS5020
7014	T42	00FCE6C	System Rack
7014	T42	00FCE7C	System Rack
7042	CR5	00DCF5B	HMC Console
7042	CR5	00DCF6B	HMC Console
7316	TF3	001525M	HMC Display
7316	TF3	001536M	HMC Display
9117	MMA	006B1D5	p770
9117	MMA	006B1E5	p770
7208	345	00U1793	EXTERNAL 8MM TAPE DRIVE
8203	E4A	00C9B51	IBM SYSTEM P 520 (BW5)
3582	L23	1311111	ULTRIUM TAPE LIBRARY
3581	H17	7805178	ULTRIUM TAPE AUTOLOADER
8203	E4A	007116	IBM SYSTEM P 520
7208	345	00U2027	EXTERNAL 8MM TAPE DRIVE
7208	345	00U0407	EXTERNAL 8MM TAPE DRIVE
7208	345	00U1816	EXTERNAL 8MM TAPE DRIVE
3582	L23	11350	LTO4 Tape Library
8203	E4A	A6D55	IBM System P 520

IBM ORACLE DATABASE

The Banner system utilizes Oracle as the database engine. The production Oracle database is stored on mirrored disk drives. In the event of a drive failure, the companion drive in the mirrored pair keeps working, thereby providing exceptional fault tolerance. Redundant disk controllers, disk power supplies, I/O channels, and Ethernet interfaces have been implemented. Further, the IBM includes a self-diagnosis and monitoring feature that warns of impending hardware problems.

Several test databases, which are a replica of the full production database are maintained. Each test database is refreshed or copied periodically from the production database. All system-critical events are evaluated on the test database prior to application to the production database.

A variety of tools to monitor and control operational conditions has been developed and is used. These tools help guide actions of the Database Administrator and protect the integrity of the database. District ITS has implemented “hot” backups using RMAN as a feature in addition to the traditional full “cold” backups. In addition, Dataguard has been installed which provides automatic database shadowing and replication between the two IBM servers.

SERVERS

The CLPCCD District ITS department manages CLPCCD’s administrative servers. These servers provide: distributed file, print, World Wide Web, Intranet, extranet, e-mail, collaboration, data archival, virus protection, and business and student administrative services for the staff and faculty. The ITS department has stayed with a heterogeneous networking strategy to leverage the strengths of each vendors’ Network Operating System (NOS). This allows broad, robust and secure networking services to all of the end users. This strategy also creates a flexible foundation at the network core on which to construct the addition of future networking services.

The main goal of the servers and the applications is to provide the administrative support and tools to the staff and faculty that are necessary for the ongoing business efforts of the colleges.

CLPCCD ITS and College computer support staff have now standardized on a server hardware platform. Hewlett Packard is the current standard server manufacturer used. Specifications are as follows:

- rack mount
- dual power supply
- hardware RAID-5
- hot swappable SATA disk drives
- dual CPU
- 8 GB memory per processor
- Minimum of 4 hard drives, 3 needed for RAID-5
- CD/DVD/BlueRay
- 2 network cards (10/100/1000)
- 2 USB ports
- 8am-5pm contract services coverage, next day, M-F

- Hard drive spares

CLPCCD District ITS staff continues to leverage the inherent values of specific operating systems to exploit their strengths for delivered functionality, ease of management and integration, security, and cost effectiveness in their environment. This requires running a network based upon open-standards to ensure maximum integration and operability between the systems. CLPCCD District ITS servers run a mix of Novell Netware, IBM AIX, Microsoft Windows 2003/2008/2012 Server, and Linux to deliver all of the core network services and applications that are required and in use on the network today.

Third party software products that provide supplemental services to the Banner System continue to be supported in partnership between the colleges and ITS. These include: (1) Sars-Trak and Stars which are products that track visits to Student Services as well as student contact hours for courses such as labs, learning resources, and tutoring to take attendance in these instructional areas, (2) Sars-Grid that tracks counseling and student scheduling contact hours, (3) Image Source software, which scans transcripts and stores the data for retrieval or updates, (4) GoPrint, a pay-for-print management system that has been installed at both colleges, primarily in the computer labs, libraries and resource centers and allows users to prepay for printed documents and provides management reporting of activity.

To improve redundancy and recoverability HP Blade Servers, HP Storage Area Networks (SANSs), and VMWARE virtualization technologies have been implemented. These systems are located in the LPC IT Building Data Center.

The following servers provide administrative services to all the district sites shown below:

Please note that for security purposes, selected charts and tables with sensitive information have been blanked out in this "general version" of the Disaster Recovery plan. This information is available for viewing upon request to the Chief Technology Officer.

Server	Main Function	Hardware	OS	Location	Description

E-MAIL/COLLABORATION

CLPCCD uses Novell GroupWise 7.0 as the e-mail and collaboration system. Users include the ITS department, faculty and administration at both Chabot and Las Positas campuses as well as the District staff. This e-mail system does not serve the student population. The District has outsourced e-mail for students using Google Gmail for the student's ZONEMAIL.

Various modules are implemented in the current setup including: Web-Access, Document Management (GWDMS), Instant Messaging (GWIM) and POP3/IMAP mail services. The ITS department is responsible for all systems maintenance, which includes but is not limited to: user mailbox management, message queue management, and enforcing the 90-day mail purge procedure which must be manually run and monitored. This latter process assures that adequate disk space is available on the mail servers for the next quarter's incoming and stored mail.

Below shows the Groupwise post offices:

Please note that for security purposes, selected charts and tables with sensitive information have been blanked out in this "general version" of the Disaster Recovery plan. This information is available for viewing upon request to the Chief Technology Officer.

Post Office	Server	IP Address	Port

For anti-Spam filtering and anti-virus, Message Architect's Netmail is deployed. The District ITS staff has standardized on the Linux and Apache-based web services.

Novell's eDirectory v8.7.3 is used for administrative authentication. This provides heightened security for all administrative network users as well as a platform for future systems integration. This system currently supports only secure authentication to Netware services. However, eDirectory was developed with the LDAP protocol and more closely parallels an industry standard LDAP implementation that other prevalent directory service implementations.

Currently Chabot, Las Positas, & the District Office are configured as Organizational Units (OU) within a single tree. The tree has both geographical and functional organizations at the root. The college OU's are broken down into functional OU's at the next level of the tree. District ITS performs directory service upgrades as needed for added functionality.

The servers that are running Netware currently are on version 6.5. Netware has a configured Single Reference timeserver. All other Novell servers act as "secondaries" and receive their time updates from this server. This is the default Novell configuration, and should function adequately with the current number of servers in this environment.

There are no major issues with eDirectory or the tree health. A health check is performed at least twice a month to ensure the DS information is replicating properly throughout the tree. The following table represents the partitioning and replica placement on the Novell servers.

MIGRATION FROM NOVELL NETWARE DIRECTORY SERVICES (NDS) TO MICROSOFT WINDOWS 2012 ACTIVE DIRECTORY SERVICES (AD)

CLPCCD has completed a major project to migrate District office users from Novell Netware NDS to Microsoft Windows 2012 Active Directory (AD). Windows AD provide network authentication and authorization services and the appropriate rights and privileges to allow users access to network resources. It is an LDAP-based directory services that centrally stores and manages network resources or objects such as user accounts, passwords, groups, security credentials, application servers, workstations, e-mail accounts, shared files and folders, and printers.

The servers that manage the Windows Active Directory are called domain controllers. The District is served with a primary domain controller housed on an HP server in LPC Administrative Computer room, and a virtualized redundant domain controller located in the Dublin District office. If one domain controller fails, users can still authenticate against the other domain controller.The domain controllers also provide internal Domain Name Resolution (DNS) and Dynamic Host Configuration Protocol (DHCP). DNS provides mapping of IP addresses to computer names internally. DHCP provides dynamic IP address to users when they log on to the network.

Additionally, printing services have been configured on print servers located in the District office at Dublin and in LPC Administrative Computer room. Printer queues and drivers are centrally stored and managed on the print servers. Users on their PCs can simply point to the print queues to print documents. If the print server located in Dublin fails, users can point to the queues stored on the LPC print server.

CHABOT AND LPC DNS AND DHCP SERVICES

Chabot and LPC provide DHCP and internal DNS services as part of the Windows Active Directory services both for instructional and administrative networks. Chabot provides internal DNS services to their instructional network with their Windows Active Directory services.

At Chabot the DNS is provided by the ChabotDCA and ChabotDCB servers. DHCP is provided by ChabotDCA. ChabotDCB is configured with DHCP and can be brought online manually if ChabotDCA fails. All desktops on the Instructional and Faculty networks point to these servers.

The Davis server provides secondary DNS for the Chabot instructional networks. Davis is queried if DNS entries are not found in the Chabot Instructional Windows ADS Domain Controllers.

At LPC, the DNS is configured on multiple servers on the Instructional network. DNS and DHCP are served by Alice (primary) and Taz (Secondary). All desktops on the Instructional, Faculty and Administrative networks point to these servers.

Iserver, Porter, and LPCDNS provide external DNS services. As CLPCCD's authoritative DNS server, this system updates the DNS servers at the ISP as to the District's externally advertised systems. It is currently running BIND 9.2 which is a secure version of DNS patched against well-known DNS vulnerabilities.

FILE SHARING

The Novell and Windows 2003/2008/2012 servers handle the file sharing for the administrative desktops. Servers are located at all three sites to handle the local users' home directories, as well as provide disk space for shared folders.

BACKUP STRATEGY

A comprehensive backup solution is essential in ensuring timely recovery of critical user information in the event of accidental deletion, hard drive crashes and corruption, security breaches, and natural disasters. Non-existent or inadequate backup capability can be very expensive due to loss of productivity, time spent re-entering data, and permanent loss of critical information.

A suite of hardware and software products have been implemented to meet CLPCCD's business continuity and disaster recovery requirements. At Chabot, LPC, and District office, Hewlett Packard (HP) high-capacity disk-to-tape and disk-to-disk hardware and Syncsort, Inc., Backup Express software has been installed.

HP disk-to-tape and disk-to-disk hardware provide the medium to backup and restore critical user data (e-mail, documents, web files, applications) to high-capacity tapes, which will be stored on-site for fast restoration and off-site for disaster recovery.

Backup Express is integrated with the HP hardware and provides a web based enterprise-level software that centrally manages the scheduling of data backups, restoration, and cataloguing of backup and restoration jobs. Backup Express supports CLPCCD's heterogeneous operating system platforms: Novell Netware, Linux, and Windows servers.

Additionally Reload software, which provides a real-time backup and restoral of e-mail messages, calendar, and appointments is deployed. Reload is capable of restoring single messages or entire mailboxes and to recover deleted e-mail in minutes.

The backup strategy uses a multi-tiered approach that enhances backup performance and optimizes recoverability when restoration is required.

The strategy is as follows:

File consolidation – Using Novell's server consolidation utility, files can be transferred at raw speeds from server to server. The utility copies entire volumes or specific directories to one or more destination servers in the same Novell eDirectory tree or in different Novell eDirectory trees. The accompanying rights, trustees, ownership and namespace information are copied to the destination server along with the files. This utility is used to move files from server to server.

Disk-to-secondary disk using virtual tape - The initial backup process will perform a disk-to-secondary disk using virtual tape. This proceeds very rapidly and immediately creates an online backup of the data. If a file is lost or deleted, it can be quickly restored from the secondary disk.

Disk-to-Tape archive – This backup method requires a transfer of the data from the Backup Disk to removable tape media. Backup to tape is usually a lengthy process, scheduled for overnight processing. As storage volumes increase, it becomes impossible to back everything up overnight. Also, if the backup fails for any reason, the staff is not onsite to perform recovery and initiate a new backup. By performing a backup from the secondary disk volume, the backups can be run during the daytime, when they can be monitored by CLPCCD technical staff.

Backup Locations - For disk-to-tape archival, tape backup hardware and software are installed at the District Office, Chabot College, and Las Positas College. Tape archival would be performed at LAN speed. For disk-to-secondary disk backup, the storage server can be located in a central location. In this case, backups could be performed across the WAN during non-business hours.

BACKUP HARDWARE

There are several hardware solutions that can be used for tape backup. LTO backup solutions are the preferred storage for CLPCCD. They offer the best storage density/performance for the size of the disks on the CLPCCD servers, with expansion for the future. The LTO units can be procured as internal or external drives to be added to the servers discretely.

Disk-to-tape:
For the District Office, the HP Ultrium 960 is deployed. For Chabot and Las Positas colleges, the HP Ultrium 960 auto loader carousels are installed. The HP Ultrium tape drive is a SCSI device that would need to be attached to a new or existing server.

Disk-to-Secondary Disk:
For disk-to-secondary disk hardware, the HP StorageWorks 1000i Virtual Library System (VLS1000i) is deployed. The VLS1000i is a disk-based storage solution that provides unattended backup and rapid restores of user data. This is accomplished by emulating a tape drive device and creating virtual tape drives stored on disks. The VLS1000i uses iSCSI (gigabit Ethernet) connectivity, and it can perform simultaneous backup of multiple servers. Restoring data from the virtual tape drives takes much less than restoring from physical tapes. The virtual tape drives stored on disk will be archived to tapes for storage offline.

BACKUP SOFTWARE

Syncsort's Backup Express software is the installed backup software. The software is YES! Certified with Novell SUSE® LINUX Enterprise Server 9, Service Pack 1 and Open Enterprise Server (OES) Linux. Backup Express offers data protection for clustered OES environments and offers more backup and recovery features for SLES and OES than any other software vendor. Backup Express includes protection for NSS (Novell Storage Services) volumes and properties on OES and SLES9 systems, and allows users to backup data on NetWare today, and restores it to OES LINUX after they migrate. While offering a superior feature set, this solution is also higher priced that other backup products.

While Backup Express is essential for backing up data stored on Novell network folders, Novell GroupWise e-mail requires a separate backup system. To backup and provide a hot spare for the GroupWise e-mail system throughout the district, Reload software is installed. Reload is a hot backup and restore solution that allows restoring single messages or mailboxes and recover deleted e-mail in minutes. Reload is specifically designed for Novell GroupWise. A dedicated

Linux-based server is required to host the software.

Backup Express is used to backup the Reload server and Linux servers used for network management.

The following table summarizes hardware and software solution suites for all sites:

Location	Hardware	Software
LPC (ITS Data Center)	• HP Ultrium 960 • HPVLS100i • HP servers(qty 2)	• Backup Express • Reload • Linux
Chabot	• HP Ultrium 960 • HP server (qty 1)	• Backup Express
DO	• HP Ultrium 960 • HP server (qty 1)	• Backup Express

BACKUP SCHEDULES

IBM Banner System: The operations staff backs up the IBM server data (including Banner) nightly Monday through Thursday incrementally with full backups performed every Friday. Moreover, the full backup done on the last Friday of the month is retained for one year. These backups are stored in the ITS operations room. The Friday night backups are taken offsite to the District office each Monday and brought back the following Monday on a rotational basis.

E-Mail and User Data: The table below shows the servers and volumes and the backup schedules:

Please note that for security purposes, selected charts and tables with sensitive information have been blanked out in this "general version" of the Disaster Recovery plan. This information is available for viewing upon request to the Chief Technology Officer.

Server Name	OS	Volume	Directories	Backup Schedule

Reload online disk-based backup software is also used to backup Email data post offices. The schedule is shown as follows:

Please note that for security purposes, selected charts and tables with sensitive information have been blanked out in this "general version" of the Disaster Recovery plan. This information is available for viewing upon request to the Chief Technology Officer.

Post Office	M	T	W	Th	F	Sat	Sun

VIII. ITS Contact Information

Chabot • Las Positas Community College District

Information Technology Services

MEMORANDUM

To: Sean Prather, LPC Safety
Antonio Puente, Chabot Safety
Tim Nelson, M&O

From: Theresa Hirstein, ITS Operations

Date: April 29, 2014

Subject: Updated ITS Emergency Call List

In the event of an off-hours emergency affecting computer service or equipment, ITS must be notified as soon as possible. Examples of such emergencies include:

Power failure, flooding
Fire, fire alarm or fire suppression system discharge
Break-in, theft, or other intrusion
Temperature alarms for LPC ITS Data Center
Or other emergency warranting immediate action

Please note that for security purposes, selected charts and tables with sensitive information have been blanked out in this "general version" of the Disaster Recovery plan. (Home phone numbers are blanked out.)

Contact	Home	Work	Alternate
Ken Agustin		925- 424-1723	
Mark Smythe		925-424-1751	
Theresa Hirstein		925- 424-1745	
Eric Stricklen		925-424-1739	
Stacey Followill		925-424-1735	
Cathy Gould		925-424-1737	
Jeannine Methe		925-424-1720 (LPC) 925-485-5213 (DO)	

When the need arises, please initiate contact with the first name on the list and continue downward until a contact is made regardless of the time of the alarm. Please leave a message on any answering machine encountered.

CHABOT COLLEGE M&O CONTACT INFORMATION

The memo below lists M&O Chabot emergency contact information:

CHABOT-LAS POSITAS COMMUNITY COLLEGE DISTRICT
MAINTENANCE AND OPERATIONS DEPARTMENT
MEMORANDUM
TO: Antonio Puente
FROM: Tim Nelson
DATE: April 29, 2014
SUBJECT: M. & O. Emergency Recall List for the Chabot Campus

Please advise your security personnel to contact the following personnel in case of an emergency at Chabot on weekends or holidays or after hours. Call supervisors first, and then work down the appropriate list, depending on the type of problem.

Please note that for security purposes, selected charts and tables with sensitive information have been blanked out in this “general version” of the Disaster Recovery plan. (Home phone numbers are blanked out.)

Maintenance Emergencies: (Heating/Air conditioning, no power, systems failure in buildings, broken water pipes, swimming pool problems, etc.)

Name	Title	Home Phone	District Cell Phone
Jim Soles	Maintenance Manager		
Chuck Bender	Maintenance Supervisor		
Miguel Angel	Maintenance Electrician		
David Hendrickson	HVAC Maintenance Engineer		
Bill Hall	HVAC Maintenance Engineer		
Robert Holleman	HVAC Maintenance Engineer		
Jesse Ellis	Hardware Specialist		

GROUNDS EMERGENCIES: (BROKEN IRRIGATION LINE, FALLEN TREES, SUPPORT FOR ATHLETIC EVENTS, ETC.)

Name	Title	Home Phone	District Cell Phone
Cord Ozment	Grounds Supervisor		
Steve Patchin	Lead Grounds Worker		
Alberto Sahagun	Grounds Mechanic		

Please note that for security purposes, selected charts and tables with sensitive information have been blanked out in this "general version" of the Disaster Recovery plan. (Home phone numbers are blanked out.)

CUSTODIAN EMERGENCIES: (SPILLS, CUSTODIAL SUPPORT FOR EVENTS, ETC.)

Name	Title	Home Phone	District Cell Phone
Richard Duchscherer	Custodial Mgr		
Royce Wood	Custodial Supervisor		
David Hernandez	Custodial Lead		
Bob Picht	Custodial Lead		

VEHICLE EMERGENCIES: (DISTRICT VEHICLES)

Name	Title	Home Phone	District Cell Phone
Rob Barattino	Maintenance Mechanic		

IF YOU ARE UNABLE TO REACH THE APPROPRIATE PERSONNEL ABOVE, CALL TIM NELSON, DIRECTOR OF MAINTENANCE AND OPERATIONS.

LPC M&O CONTACT INFORMATION

The memo below lists M&O LPC emergency contact information:

CHABOT-LAS POSITAS COMMUNITY COLLEGE DISTRICT
MAINTENANCE AND OPERATIONS DEPARTMENT
MEMORANDUM
TO: Sean Prather
FROM: Tim Nelson
DATE: April 29, 2014
SUBJECT: M & O Emergency Recall List for the Las Positas Campus

Please advise Campus Safety personnel that these are the M & O personnel that can be called in case of an emergency at Las Positas after hours, on weekends, or on holidays. Call supervisors first, and then work down the appropriate list, depending on the type of problem.

Please note that for security purposes, selected charts and tables with sensitive information have been blanked out in this "general version" of the Disaster Recovery plan. (Home phone numbers are blanked out.)

Maintenance Emergencies: (Heating/Air conditioning, no power, systems failure in buildings, broken indoor water pipes, swimming pool problems, etc.)

Name	Title	Home Phone	District Cell Phone
Jim Soles	Maintenance Manager		
Vacant	Maintenance Supervisor		
Miguel Angel Aguirre	Maintenance Electrician		
Robert Holleman	HVAC Maintenance Engineer		
Bill Hall	HVAC Maintenance Engineer		
David Hendrickson	HVAC Maintenance Engineer		
Jesse Ellis	Hardware Specialist		

Please note that for security purposes, selected charts and tables with sensitive information have been blanked out in this “general version” of the Disaster Recovery plan. (Home phone numbers are blanked out.)

Grounds Emergencies: (Broken irrigation line, fallen trees, support for athletic events, etc.)

Name	Title	Home Phone	District Cell Phone
Cord Ozment	Grounds Supervisor		
Carl Yamasaki	Lead Grounds Worker		
Ron Ribali	Grounds Worker II		
Alberto Sahagun	Grounds Mechanic		

Custodial Emergencies: (Spills, floods, custodial support for events, etc.)

Name	Title	Home Phone	District Cell Phone
Richard Duchscherer	Custodial Manager		
Don Saugar	Custodial Supervisor		
Benito (Jun) Aquino	Custodial Lead		

Vehicle Emergencies: (District Vehicles)

Name	Title	Home Phone	District Cell Phone
Rob Barattino	Maintenance Mechanic		

If you are unable to reach the appropriate personnel above, call Tim Nelson, Director of Maintenance and Operations.

IX. DISASTER RECOVERY PROCEDURES FOR IT INFRASTRUCTURE AND FACILITIES

Disaster Recovery Procedures for LAN/MAN

In the event of a disaster, LAN/WAN equipment could be damaged and become inoperable. CLPCCD standardized on Cisco network equipment. The table below lists the equipment, serial number, contract number, and the maintenance agreement purchased:

Please note that for security purposes, selected charts and tables with sensitive information have been blanked out in this “general version” of the Disaster Recovery plan. This information is available for viewing upon request to the Chief Technology Officer.

Item	Description	Serial Number	Contract	Maintenance
WS-C4506-S2+96	Catalyst 4560			
AIR-CT5508-50-K9	Wireless Controller			
WS-C4506-S2+96	Catalyst 4560			
WS-C4506	Catalyst 4560			
WS-C4506-S2+96	Catalyst 4560			
WS-C4506	Catalyst 4560			
WS-C4506	Catalyst 4560			
WS-C4506-S2+96	Catalyst 4560			
WS-C4506-S2+96	Catalyst 4560			
WS-C4506-S2+96	Catalyst 4560			
WS-C4506-S2+96	Catalyst 4560			
WS-C4506-S2+96	Catalyst 4560			
WS-C4506	Catalyst 4560			
WS-C4506	Catalyst 4560			
WS-C4506	Catalyst 4560			
WS-C4506	Catalyst 4560			
WS-C4506	Catalyst 4560			
WS-C4506	Catalyst 4560			
WS-C4506	Catalyst 4560			
WS-C4506	Catalyst 4560			
ASA5520-BUN-K9	Firewall			
ASA5520-BUN-K9	Firewall			
ASA5520-BUN-K9	Firewall			
ASA5520-BUN-K9	Firewall			

CISCO2811	Router			
WS-C6509-E	Catalyst 6509 Core			
WS-C6509-E	Catalyst 6509 Core			
WS-C6509-E	Catalyst 6509 Core			
CISCO3825	Router			
CISCO3825	Router			
WS-C6509-E-PFC2	Catalyst 6509 Core			
ACS1121	Cisco Secure Server			

If Cisco equipment and parts need to be replaced and ordered, call Cisco Technical Assistance Center (TAC) at 800-553-2447. Serial number and contract number must be provided. Cisco TAC can also assist in troubleshooting network-related issues.

Cisco IOS images and switch/router configurations are stored on data servers. If a router or switch needs to be replaced, the images and configurations can be downloaded via TFTP.

If a disaster occurs, there is also a possibility of damage to the campus fiber infrastructure. Call a cabling vendor, either SASCO or CalCoast. See vendor contacts in Appendix F which contains the list of maintenance contracts and designated contacts.

Telecommunications circuits that connect the campuses and District Office can also be impacted. If this is the case, AT&T, needs to be notified and a trouble call logged. The table below lists the circuit identification numbers of Opt-E-Man and T-1 circuits. This information is needed when calling AT&T.

Please note that for security purposes, selected charts and tables with sensitive information have been blanked out in this “general version” of the Disaster Recovery plan. This information is available for viewing upon request to the Chief Technology Officer.

Description	**Circuit ID**
LPC Opt-E-Man	
District Office Opt-E-Man	
Dublin Opt-E-Man	
Chabot College Opt-E-Man	

For Opt-E-Man outages, call AT&T at (888) 644-3662. For T-1 outages, call AT&T at (800) 332-1321.

For outages impacting the colleges’ Internet connections, call the CLPCCD’s service provider, CENIC, at (744) 220-3494 and log a trouble call.

X. DISASTER RECOVERY PROCEDURES FOR IBM/Oracle Database

The following standards are designed to reduce the mean time required to recover from service interruptions:

- **Documentation**: Copies of this plan are maintained at LPC ITS Operations Bldg 1900, room 131. Copies of all ITS-authored documentation are maintained in the Print Production room, on data servers, and on backup tapes.
- **Hardware and Software Maintenance Contracts**: ITS has contracted for maintenance service from IBM and Oracle with on-site premium service, 7x24.
- **Mutual Assistance Agreement**: The District has entered into a mutual assistance service agreement with the San Mateo County Community College District, which also uses the SCT Banner applications. The agreement pledges mutual assistance, cooperative support, sharing of technical resources, computer services, and staff resources in order to help mitigate the effects of any catastrophic failure of computer services caused by disaster at either district. Refer to Appendix A for a copy of the agreement.
- **Consulting Agreements**: The District maintains consulting services agreements with IBM, CMI, Sungard Higher Education, and Strata Information Group. Under these agreements, specialized implementation assistance can be quickly obtained when required to speed up recovery from a service interruption.
- **Technical currency**: All of the mission-critical systems operate at currently supported release levels and run on currently available hardware and unmodified operating systems. Accordingly, in the event of catastrophic loss, our database and applications can be re-implemented quickly on replacement hardware and operating systems.
- **Staff preparation**: ITS has identified a well-trained systems administrator responsible for operation of the IBM system and a database administrator responsible for managing and maintaining the Oracle database.
- **Database backups**: Several types of backups for the Oracle database are maintained:
    - Physical File Backups. These are performed weekly, monthly, and annual full backups of all file systems with the database in a “cold” or shutdown state. Nightly incremental backups of changes since the last full backup are also performed.
    - Archive logging. The production database is run in the ARCHIVELOG state to capture all transactions to a log file. Certain Oracle tools permit use of these logs to recover the database to a specific point in time, or to recover all activity since the last cold backup. This will permit recovery of all database activity up to the minute of system failure.

- Database exports. A logical export of the database is periodically done to an export dump file, which can be used to restore the database. This provides a different type of backup and a greater degree of security.
- Test database. A test database that is a replica of the full production database is maintained. It is refreshed or copied periodically from the production database. Although it is not designed as a backup tool, the test database provides an additional on-line copy.
- Database mirroring. Disk mirroring, although not sufficient as a sole backup strategy, offers an excellent recovery from disk failure and provides an additional up-to-the-minute backup copy of the production database.

Refer to Appendix B for IBM startup and shutdown procedures.

Refer to Appendix C for instructions on how to shutdown the Oracle database in an emergency.

XI. DISASTER RECOVERY PROCEDURES FOR HP SERVERS

CLPCCD has standardized on Hewlett-Packard (HP) servers running Novell Netware, Windows 2003, or Linux operating systems. These servers host critical applications such as web services, e-mail, data storage, and Banner-related applications.

Spare HP servers and hard drives have been provisioned and are readily available. Each server is configured with four hard drives or more at RAID-5 level. If one hard drive fails, it can be replaced without bringing the server down. Additionally each server is configured with dual power supplies and network cards for added redundancy.

In the event that servers or components need to be ordered, they are under warranty and service has been purchased at 8x5xNBD. Call HP technical support center at (800) 334-5144.

The table below lists the servers with the serial numbers, which must be provided to log a trouble call.

Please note that for security purposes, selected charts and tables with sensitive information have been blanked out in this "general version" of the Disaster Recovery plan. This information is available for viewing upon request to the Chief Technology Officer.

Server Name (Location)	Hardware	Serial No	Asset No

Restoration of operating system and applications software is the next step after acquiring a new server. Novell operating system and applications can be reinstalled using installation CDs. Windows server operating system and applications can be reinstalled in a two-step process. First, the core Windows server operating system is installed using CDs. Once the core operating system is installed, Windows NT Backup software, restore option, is used to recover the applications and data from tape or disk. In the future, bit-level, bare-metal recovery imaging will be used as it is more efficient and less time consuming.

Refer to Appendix D for the disaster recovery plan for each server.

E-MAIL AND USER DATA RECOVERY

E-mail and user data are recoverable using Syncsort Backup Express recovery software. The data is either restored from backup tapes or virtual tapes stored on hard disks. E-mail data can also be restored from disks using the Reload software.

Refer to Appendix E for how to recover deleted e-mails using Reload.

XII. INITIATION OF THE DISASTER RECOVERY PLAN

The preceding paragraphs detail CLPCCD's IT infrastructure and its current state of preparedness in the event of a disaster. The following sections discuss the steps that are undertaken if a disaster occurs.

The first step is the detection and determination of a disaster condition. Depending on the gravity and extent of the disaster, the proper authorities (campus police, Director of Maintenance, etc.) will notify the Chief Technology Officer (CTO) that a disaster has occurred. The CTO (or alternate) assesses the situation and initiates the Disaster Recovery Plan, invokes the phone tree, and notifies the staff members responsible for salvaging and recovering IT assets.

The CTO will identify a designated hot site where salvageable resources and spares will be moved, installed, and configured. If the LPC Data Center is severely impacted and becomes inoperable, the designated hot site will be the District Office's future backup Data Center. The CTO will manage and coordinate with the appropriate District departments the resources needed to enable the District office as a fully functioning Data Center.

The following table illustrates disaster events that can initiate the DR plan:

Event	Responsible	Severity	Cause	Action
IBM Hardware	• Ops Supervisor: Theresa Hirstein • System Admin: Eric Stricklen • Alternate System Admin: Stacey Followill	High	• Hard drive failure • Motherboard/CPU failure	• Replace failed components with available spares • Contact IBM tech support
IBM Software and Database	• System Admin: Eric Stricklen • Alternate System Admin: Stacey Followill • Database: Danita Troche	High	• Corrupted file system • Corrupted database	• Reinstall software • Restore from backup tapes • Contact Oracle or IBM

	• Alternate Database: Eric Stricklen			
HP Server Hardware	• Systems Manager: Ken Agustin • System Admin: Mark Smythe • System Admin: Revoyda Starling	Mild to High	• Hard drive failure • Motherboard/CPU failure	• Replace failed components with available spares • Contact HP tech support
Novell Data Servers	• Systems Manager: Ken Agustin • System Admin: Mark Smythe • System Admin: Revoyda Starling	Mild to High	• Corrupted file structure • Accidental erasure	• Restore from backup tapes or online disk storage • Reinstall Netware OS
E-Mail Data	• Systems Manager: Ken Agustin • System Admin: Mark Smythe • System Admin: Revoyda Starling	Mild to High	• Accidental erasure • Hard drive failure	• Restore from Reload • Restore from backup tapes
Web Server Data	• Systems Manager: Ken Agustin • System Admin: Mark Smythe • System Admin: Revoyda Starling	Mild to High	• Accidental Erasure • Hard drive failure	• Restore from backup tapes
Cable Failure	• Systems Manager: Ken Agustin • System Admin: Mark Smythe • System Admin: Revoyda Starling	Mild to High	• Accidental fiber cut • Sabotage	• Call cabling vendor (SASCO or CalCoast) • Re-terminate wiring
Data Circuit Failure	• Systems Manager: Ken Agustin • System Admin: Mark	High	• Accidental fiber cut on the WAN cloud	• Call AT&T, report problem, and log case

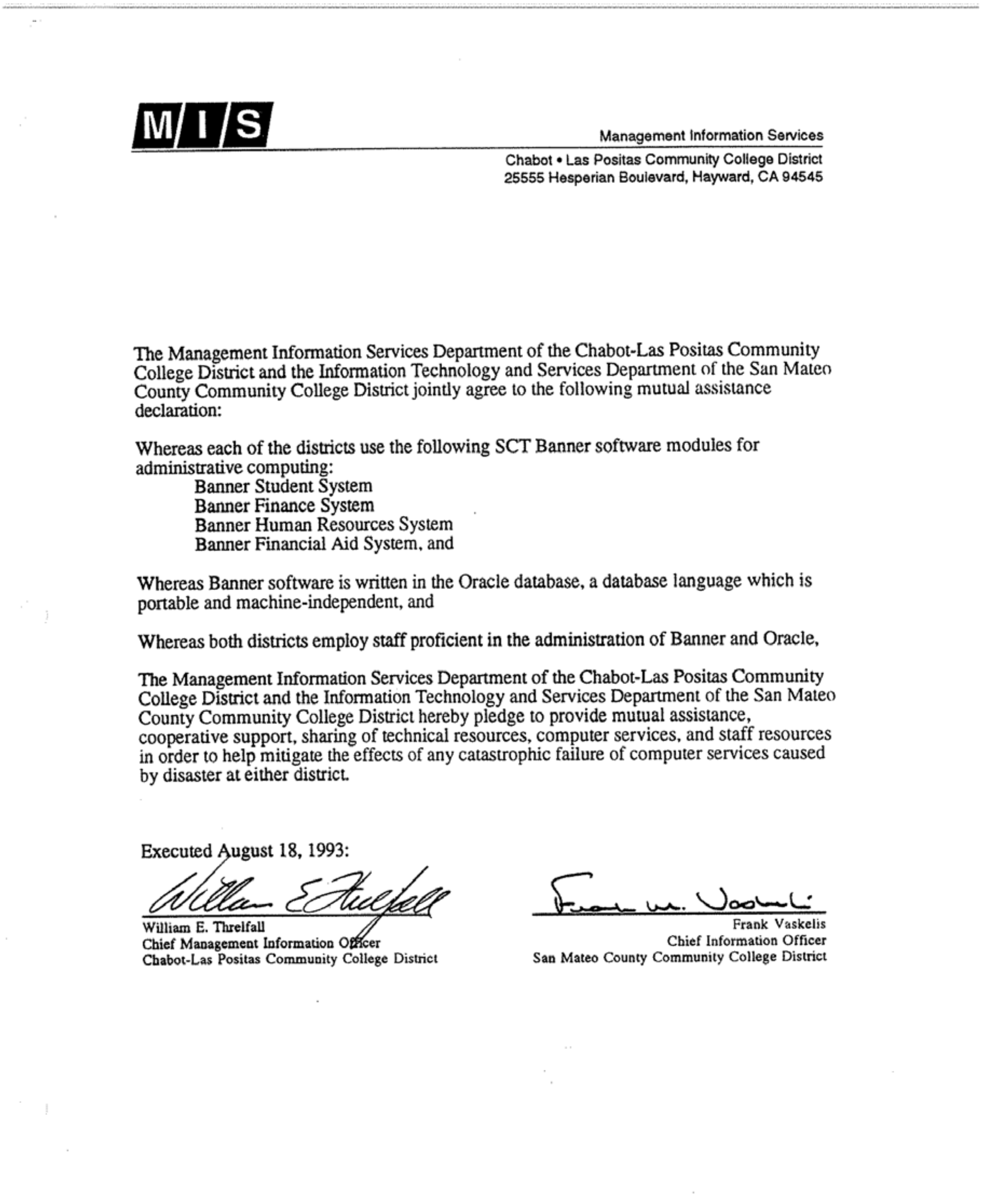
	Smythe • System Admin: Revoyda Starling		• Vendor equipment failure	
Network Equipment Failure	• Systems Manager: Ken Agustin • System Admin: Mark Smythe • System Admin: Revoyda Starling	Mild to High	• Bad power supply • Bad circuit board on switch or router • Bad fiber or Ethernet interface	• Replace failed component with spare • Call Cisco technical assistance center (TAC)
Power Outage (brief, transient)	• None	Mild	• Electrical equipment failure • Power fluctuation	• None. UPS provides line conditioning and isolation that protects equipment from electrical surges
Power Outage (1 to 45 minutes	• None	Mild	• Loss of city power • Faulty LPC electrical equipment	• None. UPS battery provides power up to 45 minutes
Power outage (46 minutes to 12 hours)	• ITS Verify remotely systems in operation	Mild to High	• Continued loss of city power • Inability to repair faulty LPC electrical equipment timely	• None. The generator automatically kicks in when UPS battery is consumed
Power outage (over 12 hours)	• ITS Refer to ITS Emergency Contact Information	High	• Continued loss of city power	• Contact M&O to fill up generator with diesel fuel
Power outage with loss of generator	• ITS Refer to ITS Emergency Contact Information	High	• Faulty generator and prolonged power outage with UPS only supplying power	• Contact M&O • Orderly shutdown of all servers • After power is restored, restart all

				servers
Main HVAC Failure	- ITS Refer to ITS Emergency Contact Information	High	- Loss of power - Faulty LPC HVAC equipment	- Contact M&O - Monitor room temperature - Secondary HVAC automatically takes over cooling the computer room
Main and Secondary HVAC failures	- ITS Refer to ITS Emergency Contact Information	High	- Loss of power - Faulty LPC HVAC equipment	- Contact M&O - Monitor room temperature - Perform orderly shutdown of all servers if temperature exceeds 85 degrees
Destruction of Computer room, servers, network equipment	- ITS Refer to ITS Emergency Contact Information	High	- Major earthquake, fire, flooding, terrorist attacks	- Initiate DR plan - See paragraph below

MAINTENANCE AGREEMENTS

A critical aspect of reconstitution when disaster occurs is the ability to summon assistance for technical expertise, troubleshooting, and shipment of spare components from the various hardware, software, and infrastructure vendors and manufacturers. Thus, it is important to ensure maintenance agreements, contracts, and licenses are up-to-date and current. Refer to Appendix F for a list of the maintenance contracts and the designated contacts.

XIII. Appendix A – Mutual Agreement



M/I/S

Management Information Services

Chabot • Las Positas Community College District
25555 Hesperian Boulevard, Hayward, CA 94545

The Management Information Services Department of the Chabot-Las Positas Community College District and the Information Technology and Services Department of the San Mateo County Community College District jointly agree to the following mutual assistance declaration:

Whereas each of the districts use the following SCT Banner software modules for administrative computing:

Banner Student System
Banner Finance System
Banner Human Resources System
Banner Financial Aid System, and

Whereas Banner software is written in the Oracle database, a database language which is portable and machine-independent, and

Whereas both districts employ staff proficient in the administration of Banner and Oracle,

The Management Information Services Department of the Chabot-Las Positas Community College District and the Information Technology and Services Department of the San Mateo County Community College District hereby pledge to provide mutual assistance, cooperative support, sharing of technical resources, computer services, and staff resources in order to help mitigate the effects of any catastrophic failure of computer services caused by disaster at either district.

Executed August 18, 1993:

William E Threlfall

William E. Threlfall
Chief Management Information Officer
Chabot-Las Positas Community College District

Frank Vaskelis
Chief Information Officer
San Mateo County Community College District

XIV. Appendix B – IBM Startup and Shutdown Procedures

Please note that for security purposes, selected charts and tables with sensitive information have been blanked out in this "general version" of the Disaster Recovery plan. This information is available for viewing upon request to the Chief Technology Officer.

XV. Appendix C – Oracle Database Shutdown Procedures

Please note that for security purposes, selected charts and tables with sensitive information have been blanked out in this "general version" of the Disaster Recovery plan. This information is available for viewing upon request to the Chief Technology Officer.

XVI. Appendix D – Server Disaster Recovery Plan

Please note that for security purposes, selected charts and tables with sensitive information have been blanked out in this "general version" of the Disaster Recovery plan. This information is available for viewing upon request to the Chief Technology Officer.

XVII. Appendix E – How to Recover Deleted E-Mail Messages

Please note that for security purposes, selected charts and tables with sensitive information have been blanked out in this "general version" of the Disaster Recovery plan. This information is available for viewing upon request to the Chief Technology Officer.

XVIII. Appendix F – Maintenance Contracts

Please note that for security purposes, selected charts and tables with sensitive information have been blanked out in this "general version" of the Disaster Recovery plan. This information is available for viewing upon request to the Chief Technology Officer.

Software/Hardware Description		License or Contract#	Expiration Date	
XL C/C++ for AIX User	IBM			
Fluke Networks Etherscope	Fluke Networks			
IBM	Chouinard & Myhre, Inc			
Chabot Microsoft Campus Agreement	ComputerLand			
LPC Microsoft Campus Agreement	ComputerLand			
Powerware UPS LPC 1900/1900A	Gruber			
Oracle	Oracle			
CurricUNET	Governet C/O Bibby Service			
Student Right To Know	State of California			
eLumen Collaborative software license	Elumen Collaborative			
Google Mail Integration	SunGard			
Blackboard Single Sign On Adapter	SunGard			
SnagIt	TechSmith			
Cobol	Micro Focus			
Fluke Networks Gold Support	Fluke Networks			
FormFusion	evisions			
Intellecheck	evisions			
Pressure Sealer	Peak Technologies			
Crystal Reports Developer/Business Objects	SAP Americas			
Netmail	Netmail			
M+Extranet	Netmail			
Novell Academic License/Zenworks	Novell			
HP8100 printer	Technic Computer Services			
7215 Printronix Band printers	Technic Computer Services			
TCP Maintenance (Student, FinAid, INAS, Finance, HR, Web for students/employees)	Sungard			
2009 Tax Year Service	Pearson Government Solutions			
Web Center Support	Internet Software Science			
Symantec Anti-virus	Symantec			
Chabot College.edu DNS	Educause			
LPC.edu DNS	Educause			
SSL	Verisign			
SMARTNET (Cisco)	AT&T			
SMARTNET (Cisco)	AT&T			
SMARTNET (Cisco)	AT&T			