Chabot – Las Positas Community College District

Information Technology Services

Disaster Recovery Plan

April 2021

Submitted By
B. Griffin
Chief Technology Officer

Table of Contents

CONFIDENTIAL APPENDICES

I. INTRODUCTION

This document provides the Disaster Recovery (DR) Plan for the Chabot-Las Positas Community College District (CLPCCD), including Chabot College located in Hayward, Las Positas College in Livermore, the EDCE site in Pleasanton and the District Office in Dublin. 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. With the remote work/learning environment required with the 2020 COVID-19 outbreak, it is now business-critical to maintain a high-performing 24x7 environment for academic and administrative work.

To fulfill the mission of high quality student education resources available 7x24x365, 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 that could compromise 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.

II. 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.

III. 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:

- 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.

- Network infrastructure includes the telecommunication circuits, firewall devices, routers, switches, and cabling.

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 threat of brush fire from the surrounding areas is also real. In past summers with fires on nearby hillsides, smoke penetration into the IT Building air supply has possibly caused premature server disk and memory failures. Arson is an unlikely, but possible, source of fire damage as well.

- Computer Crime: Internal systems are more accessible through vpn or remote web access. With the constant probes to the CLPCCD firewalls, the potential for improper access is constant. While 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. Viruses and worms can be imported from the outside causing denial of service to critical systems. There are increased incidences of email spam carrying links to external malicious websites.

IV. 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 Appendix A for "ITS Emergency Contact Information" and Appendix B for "M&O Emergency Contact Information" for both Chabot and Las Positas Colleges.

V. IT INFRASTRUCTURE

CLPCCD ITS houses computer systems, telecommunications, and data networking equipment in many buildings across the CLPCCD sites, including:

- LPC IT building 1900 in Livermore
- LPC building 1900A in Livermore
- Chabot building 200 in Hayward
- Chabot building 300 in Hayward
- District Office Server/Network rooms in Dublin.
- EDCE network room in Pleasanton

These locations are equipped with the most robust technology feasible to ensure continued operation. Each of the primary facilities is discussed in more detail below.

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

The center of CLPCCD ITS' server/data infrastructure is located in the 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, including Luminus, DegreeWorks, electronic mail, file storage, DNS/DHCP/AD, Intranet and Internet web services, and network management tools.

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

As part of the construction of the LPC IT building, a number of sophisticated HVAC control, Power, and Control and Monitoring systems were designed to provide a robust operating environment with 24x7 operation.

HVAC Control

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

- **Air Handler Unit (AHU-2A):** This supplies the heating/cooling for the Administrative Data Center, LPC Instructional Server room and the IT Building Network room. This unit is supplied from the Central Utility Plant (CUP). This system provides cooling to maintain an operating temperature of 72 degrees F.

- **Air Handler Units (AHU-2B):** This unit is a second unit that also supplies heating/cooling for the Administrative Data Center, LPC Instructional Server room and the IT Building Network room. This unit is also supplied from the Central Utility Plant (CUP). This unit is also active and takes over if a failure of the AHU-2A occurs.

- **Supplemental 5 Ton System:** In addition to the AHU systems, a ceiling mounted HVAC system is installed in the Administrative Data Center. 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, as action is taken to restore the Data Center to its normal operating temperature.

- **Redundant CUP infrastructure:** The CUP is designed and built with redundant pumps, chillers and other infrastructure to ensure uninterrupted operation. Within the CUP, the control systems rotate the use of the devices so that hours of operation are balanced.

The water source for the HVAC systems comes from the Central Utility Plant (CUP). The CUP is equipped with three chillers. CUP pumps operate 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 system operates from 6am to 10pm. If ice is not available, the chillers run to maintain the cold water supply. At 10pm, the system shuts down to make ice. A heat exchanger (HX3) comes in to operation to supply cooling to the IT building. while the rest of the CUP is in ice-making mode. During ice-making mode, the chillers initiates back into service as needed to supply cold water.

If 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:

- Temperature of the Server room(s) air is too high.
- CUP chillers fail.
- Power failure on campus which takes down the CUP equipment.
- EMS panel in the IT building detects a CUP malfunction.

Except for planned power outages needed for maintenance and/or construction, it is not expected that the Backup Chiller would run regularly. Proactively, if there is work scheduled in the CUP, or a planned power outage, M&O switches the IT Building to run on the Backup Chiller. This is done to ensure a stable cooling environment for the server rooms.

Power for Building IT Building Server and Network Rooms

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

The Administrative Data Center houses Eaton Powerware UPS systems for power-protection. The systems installed 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 Data Center. 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 power to the LPC Server Room, Network room, and the remaining Administrative Data Center. It connects to the electrical panels UR2-4, which serve the electrical circuits to the rooms just listed, and a select number of power outlets in certain offices in the IT building.

The UPSes are maintained annually by a service contract which includes quarterly preventative maintenance (PM) appointments, battery and equipment checks. Batteries are replaced according to a schedule provided by the maintenance provider and manufacturer.

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 supplies the generator with diesel fuel. In the event of a power failure, an automatic transfer switch (ATS) senses the lack of campus power and triggers 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 Server 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 ensure correct functionality.

As of electrical upgrades to the IT Building executed early in 2020, the entire LPC IT Building operates on generator power during an electrical outage on campus. This allows ITS and LPC Technology staff to continue working from their office spaces as the disaster/outage is addressed.

LPC BUILDING 1900A MPOE/MDF

The LPC Campus has a centralized network and telecommunications facility that houses the carrier (AT&T, Verizon) and CENIC telecommunication equipment. This is essential for campus network connectivity, the telephone system communication and the campus Distributed Antenna System (DAS). These facilities contain the DAS equipment, 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. Robust power and HVAC systems are installed in this building, as described below.

HVAC Systems

In Building 1900A, a series of 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 (2) 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. This building is typically maintained at a temperature of 68 degrees F.

Power Systems

Building 1900A has been equipped with an 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. In the event of a power outage on the campus, this UPS keeps the equipment powered until the generator restores power to the building.

CONTROL AND MONITORING FOR LPC BUILDINGS 1900 AND 1900A

There are several levels of control and monitoring:

- **Temperature Alerting** – In each of the LPC Server room, Administrative Data Center and B1900A MPOE/MDF, temperature sensors are installed. These sensors are connected to the network and set for alerting at a maximum of 78 degrees F and minimum of 60 degrees F. When temperatures outside of the normal range occur, the sensor sends an email to a group distribution list of IT and M&O staff which alerts cell phones and emails of the temperature issue.

- **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 Data Center. 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). The UPS also send status messages for internal self-tests, which confirms that the communication from these units is still working.

- **Security Monitoring -** The AMAG security system monitors temperature probes in the Network room and Administrative Data Center 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 by the M&O staff.

- **Fire Suppression** – The B1900A MPOE/MDF and B1900 the LPC Server room and Admin Data Center are equipped with the Inergen Fire Suppression system for rapid extinguishing of fire. This system is maintained with preventative maintenance visits and annual testing to ensure it correctly operates.

- **TempAlert monitoring** - In addition to the systems described above, each room is equipped with an independent TempAlert monitoring system. This has temperature probes suspended at the air in-take of specific racks. This system flags temperature abnormalities by forwarding an email to a distribution list that texts staff cell phones of the situation.

Since many of these alerts are generated by HVAC 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.

SERVER ROOM AT CHABOT COLLEGE

The B300 Server room provides a robust environment for Chabot College servers and CLPCCD District Internet servers. This consists of:

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

- Network room – The current network room (MDF) is equipped with 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.

- Fire Suppression – The Network and server rooms are equipped with the Inergen Fire Suppression system for rapid extinguishing of fire. This system is maintained with preventative maintenance visits and annual testing to ensure it correctly operates.

- UPS – The 45KVA UPS provides power to both the network and server rooms. 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.

- Generator – A 150 KW generator provides power to the B300 server and network room equipment during power outages. This generator is sized to run a minimum of four hours before refueling. Maintenance and refueling of the generator is provided by Chabot M&O. Weekly tests and scheduled maintenance checks ensure that the generator is operating properly.

The B300 server room contains standalone District servers for 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.

Campus telephone and voicemail systems are also located in the B200 MPOE. The campus telephone system is an Avaya system with AVST voicemail. Housed in B200, the MPOE equipment is supported by a 30KVA UPS, and 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 in B200 is also powered by the 30KVA UPS for sustained uptime during power outages. On an exception basis, a portable generator can be wired into the electrical panels of B200, for sustained power during extended and planned outages.

While a key point of connectivity for the campus, this room is out of space and cannot sustain further connectivity. In addition, B200 is planned for demolition as part of a future construction project. As such a new MPOE has been built.

CHABOT COLLEGE NEW MPOE

A construction project completed in 2020 has built a new MPOE/MDF room in B307. This room has been provisioned with new conduit connections to the campus loop, and AT&T vaults. The room houses racks and termination space for:

- Fiber data connectivity from campus buildings
- Campus data network equipment
- Copper voice connectivity from campus buildings
- Campus telephone system
- Carrier connectivity (fiber/copper)
- Distributed Antenna System equipment and connectivity
- District servers, including space for a redundant Banner system

This room is provisioned with its own 50KVA UPS, HVAC and Novad fire suppression system. The UPS is connected to the existing generator servicing the other network and server rooms. With the available space and capacity, it is expected that this new MPOE/MDF room will provide robust and reliable connectivity to Chabot campus for the foreseeable future.

EDCE NETWORK ROOM

The CLPCCD EDCE department has moved to a new site in Pleasanton. It has a dedicated IDF room which houses the data, telephone and security systems for the site. All critical equipment is UPS-protected. Since this site occupies one floor in a multi-tenant building, it relies on building security for limited, authorized access to the floor. The IDF is only accessible to select personnel, by key.

DUBLIN SERVER/IDF ROOMS

At the District office location in Dublin, the third floor houses a server room which contains servers for print and file services for the District Office users. These servers are connected on UPSes to allow up to 30 minutes of uptime, thereby facilitating a clean shutdown of the applications before the UPS batteries drain.

VI. NETWORK INFRASTRUCTURE

CLPCCD operates networks that provide data connectivity inside and between CLPCCD locations.

LAN (LOCAL AREA NETWORK)

All CLPCCD sites are provisioned with Cisco routing and switching products to serve as the respective core 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 aspects of this new network architecture are as follows:

- High Availability: CLPCCD has incorporated 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 1) a Cisco Catalyst 6509 router/switches with and intelligent engine modules and redundant power supplies and 2) up to two (2) Cisco 9500 router/switch for distributed routing and VLAN control.

- Security: The networks are segmented 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 usage basis. At the campuses, CLPCCD uses a dual firewall architecture with an outward-facing firewall that provides VPN and Internet controls, and an inside firewall to segment the different security zones inside each site.

- 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. All major buildings at the campuses are connected on a 10G interface, for high bandwidth access to campus servers and the Internet.

- Redundant Server Connectivity: Wherever possible, multiple 10G connections to mission-critical servers by using dual network interface cards have been installed to limit downtime caused by NIC card failures.

- Manageability: The architecture is built upon consistent hardware platforms and software configurations, using standard routing protocols. 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 6509/9500 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 3650 switches.

At the Chabot Campus, the switches are connected to new or renovated buildings using single mode fiber with 1000Base-LX connectivity. 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. 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.

Each campus is provisioned with Primary and Secondary wireless controllers for support of campus-wide 802.11ac wireless. Where possible, wireless controllers are located in different buildings, connected to different switches, to allow for additional resiliency in the event of a switch failure.

For the essential LAN routers and switches, wireless controllers and firewalls, 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 3650 switches, ample spare parts are available and ready to be deployed as necessary.

AT&T ASE NETWORK

CLPCCD operates connections between all of the CLPCCD sites, using the AT&T ASE network, based on Ethernet over fiber. This provides high performance connectivity for access to the Administrative Data Center where centralized applications like Banner, email and file storage are located. AT&T designs its ASE network with redundant connections and failover recovery. This is managed outside of the scope of CLPCCD operations.

Below is an illustration of the CLPCCD ASE Network:

Any site provisioned with an ASE network connection, can access any other CLPCCD site, if security permits. This allows the rerouting of internet connectivity, should a campus Internet connection fail.

INTERNET CONNECTIVITY

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, ten Gigabit (10G) of network connectivity for each college has been provisioned. Also, CENIC has provisioned transparent failover connectivity and rerouting should the primary Internet connection fail.

In this topology, should a default link at either campus fail, the Internet traffic would be transparently rerouted to through the Internet connection at the other campus.

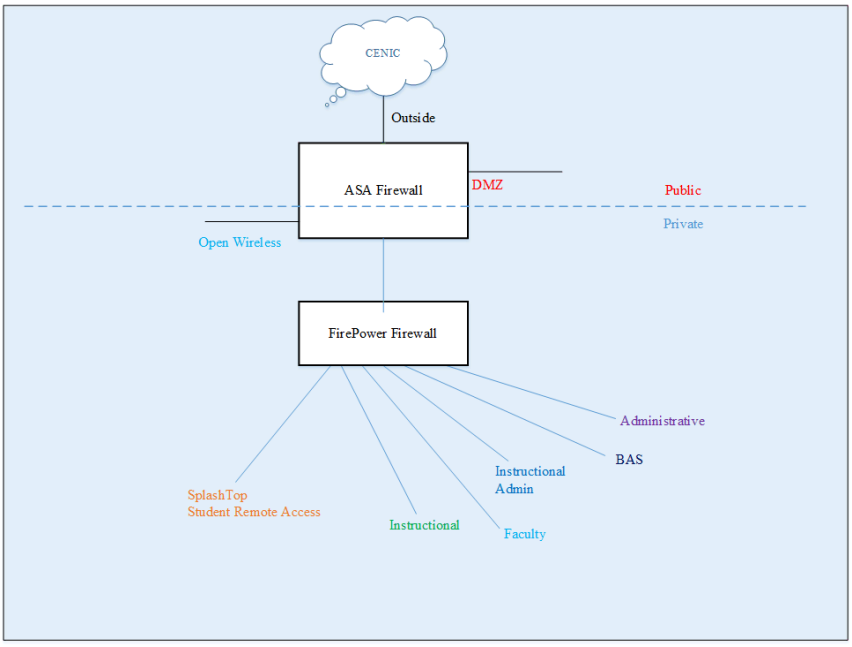
FIREWALLS

To secure the Internet connectivity for the campuses, Cisco ASA 5585 firewalls were installed in 2017 as an upgrade to the Cisco 5520 firewalls. This provided 10G connectivity for CENIC and internal network connectivity.

Each campus has a pair of ASA 5585 firewalls, equipped with multiple Ethernet interfaces and 10,000 VPN licenses. 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. The ASAs provide security for the following zones:

- External interface – public IP, facing the Internet
- Internal interface – private IP, facing the campus network
- Instructional/Admin DMZ – public IP, with servers accessible from the Internet.
- Wireless interface – private IP for campus open wireless

Internally to each campus, CLPCCD has installed Cisco Firepower firewalls, also in a Primary/failover configuration. These are architected to provide multiple security zones for campus vlans.



This architecture provides more control and analysis of traffic. It also provides for more robust failure recovery if one set of firewalls were to become compromised in any manner.

The Cisco firewalls have Cisco SMARTNET maintenance support at 7x24x365, 4-hour response time.

VII. 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, new MPOE and District ITS/Campus server rooms are located in locked areas in Chabot building 300. Cameras and the college computer staff monitors access to these rooms. The area is protected with two factor authentication with card key and keypad access. Security alerts are 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. Two factor authentication with 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. As buildings have been renovated and modernized, network equipment is 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.

Passwords

District ITS department maintains three separate user accounts. This includes Active Directory (AD)/email accounts, 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 AD/email passwords on a regular basis as needed. AD/email password recommendations are: 8 or more characters with a mixture of numbers, lowercase/capital letters and a special character.

At Chabot, Instructional Active Directory passwords are managed by the Chabot Computer Support staff. AD/email password recommendations are: 8 or more characters with a mixture of numbers, lowercase/capital letters and a special character. Password expiration has been suspended during the COVID work from home time period.

At LPC, Instructional Active Directory passwords are managed by LPC Technology Support staff. Passwords need to be changed every 180 days or as prompted, using a local workstation on campus or Outlook Web. The password format is:

1. Minimum of eight (8) characters.
2. The password must contain a minimum of three of the following four types of characters:

    a. lowercase letters;
    b. uppercase letters;
    c. numbers;
    d. !, @, #, $, %, ^, &, | : ; " ' < > , . ? /

3. The same password cannot be used for at least three changes.
4. You cannot use any part of your first name, last name or institution name in the password

Network device passwords for routers and switches are also maintained by the District ITS department and changed as needed to secure access. Passwords are individually set for each staff person who is authorized to access the network equipment. Switches have a user level logon to allow Chabot and LPC computer support technicians to execute a limited set of commands, such as modifying VLAN assignments as needed at each campus. Logons with username are recorded in the device logs.

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.

CLPCCD and the colleges have just recently changed to Sophos Anti-virus. Sophos is installed on all desktops and laptops. Anti-virus definitions are provided directly from the Sophos website. Sophos tracks and monitors user activity, including malicious activity on websites, viruses, etc. Reports, customized for each site, are provided so a detailed analysis of virus and threats is readily available.

VIII. 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)
- Argos (queries and reporting)
- Degree Works
- R25Live Room Scheduling
- Document Management System (BDMS)

There are two IBM servers, purchased and installed in the Administrative Data Center. They are running IBM's Virtualized environment. Hardware and software configurations are replicated so either server can operate as the primary Enterprise server. Oracle database and user data are stored on the primary server and can be 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 virtual servers for CLASS-Web services and Internet Native Banner (INB). As virtual servers, the CLASS-Web and INB servers have hardware redundancy and application redundancy for backup in the event of an unexpected failure.

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.

IX. HP 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 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 standardized on a server hardware platform. Hewlett Packard is the current standard server manufacturer used. Specifications vary with procurement but conform to the following reliability guidelines.

- rack mount
- redundant power supplies
- hardware RAID-5
- hot swappable SSD disk drives
- multiple CPU
- 16 GB memory per processor
- Minimum of 4 hard drives, 3 needed for RAID-5
- multiple network cards (100/1G/10G)
- USB ports
- 24x7x365 response center contact, 4 hour onsite response time

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 is based upon open-standards to ensure maximum integration and operability between the systems. CLPCCD District ITS servers run a mix of IBM AIX, Microsoft Windows 2012/2016 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 which is product 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 provisioned in the Administrative Data Center, LPC Server room and Chabot Server room.

E-MAIL/COLLABORATION

CLPCCD uses Microsoft Exchange as the e-mail for faculty and administration staff at all sites. 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.

The Exchange system consist of a front-end load balancer which gives access to multiple back-end mail stores containing the users' mailboxes. Mail can be accessed using the Outlook client or using the Outlook Web Access (OWA) interface. Though the OWA interface is less functional, it is available to users on or off campus. The Exchange calendaring system is also used.

The ITS department is responsible for all systems maintenance, which includes but is not limited to: user mailbox management, message queue management, etc. CLPCCD uses the Barracuda Mail filter hosted service to filter inbound email and flag suspicious mail for quarantine. Filtering is performed on a per-message and per-inbox basis allowing users to confirm if a suspicious message is spam or valid.

CLPCCD ITS is in the process of migrating to O365 and Microsoft hosted Exchange. This will provide more functionality and resiliency. It is expected that the migration will complete in 2021.

WINDOWS ACTIVE DIRECTORY SERVICES (AD)

CLPCCD has uses Microsoft Windows 2012 Active Directory (AD)to provide network authentication and authorization services and the appropriate rights and privileges to allow users access to network resources.

Servers that manage the Windows Active Directory are called domain controllers. The District has multiple domain controller housed in LPC Administrative Data Center and the Dublin District office. If one domain controller fails, users can still authenticate against other domain controllers. The domain controllers also provide internal Domain Name Resolution (DNS) and Dynamic Host Configuration Protocol (DHCP).

Additionally, printing services have been configured on print servers located in the District office at Dublin and in LPC Administrative Data Center. 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 provide DHCP and internal DNS services as part each campus' discrete Windows Active Directory forest. All desktops on the Instructional and Faculty networks point to the server(s) for their respective campus.

Iserver, Porter, and LPCDNS provide external DNS services. As CLPCCD's authoritative DNS servers, these systems update the DNS servers at the ISP as to the District's externally advertised systems. It is currently running BIND 9.9.9-P1 which is a secure version of DNS patched against well-known DNS vulnerabilities.

FILE SHARING

Windows 2012/2016 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 SYSTEM

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.

For backup of Windows servers, CLPCCD has standardized on Unitrends Linux based backup and recovery appliance with Web UI. Each of the district sites and the colleges have a separate Unitrends appliance which they configure for unique schedules.

District Server Backup

The backup system at for the District office servers utilizes 65TB Unitrends Linux based backup and recovery appliances with Web UI. An appliance is on premises and located in the Administrative Data Center. A second appliance is located in the District Office server room, for backup of the servers at that site.

Servers are backed up daily on either a full & incremental plan or incremental forever plan determined by data and/or service provided.

Unitrends appliance notifies District staff of backup failures and logs by email daily.

- Servers performing file level backups minimum retention of 45 days
- Servers providing software services minimum retention of 45 days
- Database Servers minimum retention 90 days
- File Servers backup minimum retention 90 days
- File servers with Institutional and Sensitive Data 365 day minimum retention

Chabot College Server Backup

The backup system at Chabot College utilizes a 65TB Unitrends Linux based backup and recovery appliance with Web UI. This appliance is on premises and located in the Chabot Server

Room. Servers are backed up daily on either a full & incremental plan or incremental forever plan determined by data and/or service provided.

The Unitrends appliance notifies Chabot staff of failures by email. Logs reviewed several times a week.

- Servers performing file level backups minimum retention of 45 days
- Servers providing software services minimum retention of 45 days
- Database Servers minimum retention 180 days
- File Servers backup minimum retention 180 days
- File servers with Institutional and Sensitive Data 180 day minimum retention

Las Positas College Server Backup

The backup system at Las Positas College utilizes a 65TB Unitrends Linux based backup and recovery appliance with Web UI. This appliance is on premises and located in the LPC Server Room – 1942. Servers are backed up daily on either a full & incremental plan or incremental forever plan determined by data and/or service provided.

Unitrends appliance notifies all members of LPC IT staff of failures by email. Logs reviewed weekly at minimum.

- Servers performing file level backups minimum retention of 30 days
- Servers providing software services minimum retention of 30 days
- Database Servers minimum retention 90 days
- File Servers backup minimum retention 180 days
- File servers with Institutional and Sensitive Data 365 day minimum retention

Detailed information about the backups are provided in the Appendices.

Banner Backup

The Banner servers are backed up to tape on a detailed schedule of full and partial backups. Tapes are rotated and taken offsite each week. In addition to the tape backup, the systems are backed up to Amazon Web Services (AWS) in the cloud. This provides for double redundancy in the even that a backup need to be access for file recovery.

X. 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.

If the Administrative Data Center at LPC becomes unusable, the CTO will identify a designated hot site where salvageable resources and spares will be moved, installed, and configured. The CTO will manage and coordinate with the appropriate District departments the resources needed to enable the designated hot site 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: Cathy Gould • 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: Cathy Gould • Alternate System Admin: Stacey Followill • Database: Danita Troche • Alternate Database:	High	• Corrupted file system • Corrupted database	• Reinstall software • Restore from backup tapes • Contact Oracle or IBM
HP Server Hardware	• Systems Manager: TBH • System Admin: Steven McGervey	Mild to High	• Hard drive failure • Motherboard/CPU failure	• Replace failed components with available spares

	• System Admin: Revoyda Starling			• Contact HP tech support
Data Servers	• Systems Manager: TBH • System Admin: Steven McGervey • 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: TBH • System Admin: Steven McGervey • System Admin: Revoyda Starling	Mild to High	• Accidental erasure • Hard drive failure	• Restore from Reload • Restore from backup tapes
Web Server Data	• Systems Manager: TBH • System Admin: Steven McGervey • System Admin: Revoyda Starling	Mild to High	• Accidental Erasure • Hard drive failure	• Restore from backup tapes
Cable Failure	• Systems Manager: TBH • System Admin: Anthony Seung • 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: TBH • System Admin: Anthony Seung • System Admin: Revoyda Starling	High	• Accidental fiber cut on the WAN cloud • Vendor equipment failure	• Call AT&T, report problem, and log case
Network Equipment Failure	• Systems Manager: TBH • System Admin: Anthony Seung • 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 continuity until the generator restores
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,	• ITS Refer to ITS Emergency Contact Information	High	• Major earthquake, fire, flooding, terrorist attacks	• Initiate DR plan • See paragraph below

network equipment				

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.

Documentation for Maintenance Contracts for IT hardware and software are maintained in a Access database by the CLPCCD ITS Executive Assistant. In this database the following information is available:

- Company name
- Products covered
- Support Contract life span
- Contact name and phone number

Separate documentation is maintained with the current and historical purchase record details, so that a complete set of information on any product is available electronically. This documentation is available as needed to District ITS, Chabot College and Las Positas College staff.

Appendices

CLPCCD ITS Confidential