Pleasanton Unified School District

Technology Services
Disaster Recovery Plan
2019-2022

Table of Contents

Part 1: Introduction

The purpose of this document is to outline the steps that will be taken to ensure the continuity of information in the event of a disruption to database applications, telecommunications or network services that would prohibit or limit access to key organizational information.

This plan will define specific activities that will be undertaken during the defined plan years (2019-22) to create a more resilient technology infrastructure. This document is not a comprehensive Business Continuity Plan, but is intended to define the activities that will be undertaken to manage the District's exposure to lost productivity that would occur in the event of potential disasters that could cause an interruption in access to network service or database applications.

Comprehensive recovery strategies for specific systems or services are not included in this document. This document will outline the timeline and framework that will be utilized to create, define and test recovery strategies for core district information systems.

Scope of Plan:

IT systems are typically comprised of hardware, software, data, staff and physical facilities. These components work together to ensure that staff and stakeholders are able to access organizational information. Information is stored as data in a variety of different servers and services, and is accessed from computer networks.

Disasters that can compromise data stored on servers or can limit access to the network are typically caused by one or more of the following types of disaster scenarios:

- Power outages
- Fire, flood or other natural disasters
- Human error
- Malicious human activity (malware, theft, vandalism)

Preventative actions can be taken to create a network environment that will create options for disaster response. In order to effectively plan for disaster response, technology systems should be individually assessed to determine the potential impacts of disaster scenarios, and to outline the corresponding risk mitigation strategies and/or the recovery/restoration steps that will be utilized in the event of a disaster.

This plan includes two sections. The first section will provide an outline of the preventative efforts that will be undertaken to provide a resilient network and data infrastructure during the scope of the plan, and the second section will identify the risk assessment methodology that will be used to plan and document disaster response and recovery activities for district systems.

Part 2: Network and Data Resiliency

Current Data Center Environment

District Technology Services server and network hardware and services are located at the District Office data center. Appendix A provides a summary listing of the District's information systems.

The District utilizes virtual server hardware infrastructure to store and operate more than 70 servers that provide information and network services to staff, students and community members in the district. These resources are backed up to data storage systems that provide local and off-site "cold" storage (ie. in order to be accessible and usable, the data has to be copied back to the primary server hardware system). The district owns and maintains all server hardware infrastructure, and leases the data backup appliance that backs up data locally and offsite.

Internet services are obtained from the K-12 High Speed Network node located at the Alameda County Office of Education. Network access to these resources, including the district-wide internet services, is provided via leased wide area network (WAN) connections to all district sites. These WAN services are currently leased from AT&T, and are partially funded using e-Rate subsidies. The District owns and maintains all infrastructure that provides local area network (LAN) access in each district facility.

Telecommunications services, including landline telephone and voicemail systems, are provided using a mixed environment of servers located at each district site. Telephone connections outside the district are provided using analog phone line services obtained from AT&T.

The Measure I1 bond will fund the District's transition to network based Voice Over Internet Protocol (VOIP) telecommunications services during the life of this plan. VOIP will utilize the same district-owned server and network infrastructure that is currently being utilized for all other District technology services External telephone connections will continue to be provided by a telecommunications vendor (such as AT&T). The types of connection services will be modified to support VOIP.

Cloud vs Premise Systems

Pleasanton USD utilizes a hybrid of cloud and premise systems. Many of our organizational information assets are now stored outside of the District's physical facilities in servers that are maintained by vendors and other agencies - "cloud systems". "Premise systems" are stored inside the District's facilities in the server hardware located at the DO and maintained by Technology Department staff.

Disaster recovery efforts for cloud based services can vary from those that are employed for "premise" based systems. Disaster recovery planning for premise and cloud systems requires ensuring that there are resources available to store redundant backup copies of data, and that the backup copies can be accessed as information if the primary data sources are rendered unavailable due to a disaster scenario. Because information is stored outside of the district's network, disaster recovery planning for cloud systems and, eventually, VOIP will also require ensuring that there are alternative network pathways to access data if primary network pathways are rendered unavailable due to a disaster scenario.

Improving Network and Data Resiliency

In order to provide an environment that will allow for rapid recovery during a disaster scenario, the District plans to implement a variety of measures during the life of the plan:

- Implement a disaster recovery site that will provide for redundant network services and data servers
- Upgrade district-wide data backup systems
- Implement additional backup power capabilities at the primary and disaster recovery sites

Disaster Recovery Site

The core of our district-wide network and all premise based district servers are stored at the District Data Center located in the District Office campus. In the event of any sort of disaster or power outage that affects that physical facility, all district technology systems can be negatively impacted up to and including full inaccessibility. Because this location creates a significant "single point of failure", a key objective of this plan is to create a redundant facility that will provide real-time, live backups of all premise servers and a backup internet connection.

Administration intends to implement this Disaster Recovery Site in two phases: The first phase will provide the infrastructure that will allow for live, real-time server replication. The second phase will provide services and infrastructure that will allow for a redundant core network, including internet access.

Data Backup Systems

District data stored in premise database applications (including the servers themselves) are currently backed up to a system that includes premise based and cloud storage. The system is effective for ensuring that data is available if lost, however, the speed of the system is slow. In practice, this means that data recovery is possible, but slow.

Administration plans to upgrade the data backup system by installing a new system that will increase the network transfer speed for backups and recovery for both the premise and cloud based data backups.

Backup Power Capabilities

There are a variety of solutions for providing backup power to server and network infrastructure in the event of an interruption in the main facility electrical systems. Short term power can be provided using Uninterruptible Power Supplies (UPS), which rely on batteries to provide power. Longer term power can be provided using generator systems that will produce small quantities of electricity locally in our facilities using some type of fuel source (diesel or natural gas).

During the life of this plan, the Administration intends to undertake an investigation of potential solutions, including obtaining cost estimates, for the variety of solution options that may be possible to provide alternative power in the event of a power outage of the main electrical service. Funding is not identified for these solutions at this time.   Depending on the total costs for these solutions, it may be possible to fund these solutions as part of the Measure I1 VOIP project.

Part 3: Risk Assessments & Disaster Response Procedures

Risk Assessment: Evaluating Risk Impact and Establishing Mitigation Strategies

In order to effectively plan for information system disaster recovery, Technology Department staff need to have an understanding of the types of problems that can limit or prevent needed access to information as a result of disaster, and need to define the steps that will be taken to respond to and recover from particular disasters that may occur. Advance planning and documentation can ensure that staff can efficiently proceed with recovery actions in the event of a disaster.

Risk Impacts

Disasters scenarios can cause interruptions to network services or loss of data. Disaster scenarios can be localized or widespread. They can impact multiple district locations, or limited to single sites, buildings or individual system components. Different scenarios can result in different types of risks to network services and data. This section will outline the typical risks that are associated with different types of disaster scenarios.

Fire / Flood and Other Natural Disasters:

Natural disasters such as fire and flood can damage the electronic hardware that stores data or that provides network access to data storage servers. Response to this type of damage generally includes the replacement or repair of the damaged hardware and the restoration of the data to the repaired or replaced system. The use of redundant systems that provide replacement systems that are immediately available when primary systems fail is a method of ensuring rapid recovery from disaster scenarios.

Human Error and Sabotage:

Hardware and electronic data can be subject to damage or destruction via human error or sabotage. Sabotage activities can include the introduction of malware or theft of hardware or information assets. Prevention of these sorts of activities is managed via comprehensive Information Security strategies. Those strategies are outside of the scope of this document, and should be outlined in a corresponding Information Security plan that is adopted and utilized by District Technology department staff to prevent incidents from occurring and to manage response to information security breaches.

When systems or data are damaged or compromised due to information security breaches or other instances of human error or sabotage, recovery efforts are identical to those that are outlined in the prior section (Fire / Flood and Other Natural Disasters).

Power Outage:

A loss of power can disrupt both the storage of and access to information by entirely disabling electronic network and server systems. Typically, recovery is either postponed until the primary electrical service is made available or alternative backup power service is utilized until the primary electrical service comes back online.

Risk Mitigation Strategies

The response to different types of disasters may vary for different information systems depending on the relative priority of the information or service that may be affected and the nature of the impact.

Disaster Recovery Site

By implementing a "hot" disaster recovery site, the District will be able to establish routine procedures to backup data and network services so they can be made accessible to district stakeholders rapidly in the event of damage to the primary District Office data center. Mission critical servers and network systems will be backed up from the DO data center to the disaster recovery site and made available on server hardware systems that can operate in lieu of the primary District Office data center servers in the event of a disaster.

Data Backup and Restoration

Hot disaster recovery can be an expensive proposition, as it essentially requires that the district support dual server and network systems. Some systems and information benefit from additional version backups, or do not require real-time backup and restoration capabilities. In order to manage costs required for these types of backup, "cold" data backup and restoration strategies will also be implemented. "Cold" data storage simply holds copies of data backups, and doesn't provide methods to actually operate the servers and systems that are copied.

Redundant Network Connections

Network access is provided via a complicated "web" of connections that is arranged in a hub and spokes model centered at the District Office data center. Internet service is brought in from the ACOE to the DO data center, and is essentially distributed to all district sites by being just another hub and spoke in the web of network connections. In order to ensure continuity of network services in the event any of the site-based connections, or the core DO connection, is compromised, the District can design and implement network redundancy by obtaining and configuring additional internet and WAN connection services that would be utilized in the event of failure of the primary connections.

Alternative Backup Power Solutions

Interruptions in power service can be mitigated by installing alternative backup power solutions. Potential alternative backup power solutions can include uninterruptible power supply (UPS) systems and generators. UPS systems use batteries to provide alternative electricity. Generators use a diesel or natural gas fuel source to generate small quantities of electricity for a single facility.

Alternative backup power systems are typically directly wired to district systems by selecting hardware that can incorporate dual power connections -- one cable is connected to the main electrical service, and the other cable is connected to the alternative backup power service. In the event of interruptions to the primary electrical service, systems can automatically begin to use (aka "failover to") the alternative backup power system. Systems that lack options for dual power connections will require human intervention to establish new physical connections to the alternative backup power system in the event of interruption to the primary electrical service.

Disaster Recovery Procedure Testing

In order to provide the smoothest possible response in the event of a disaster scenario, staff will plan and document the procedures required to bring backup server, network or electrical systems online if primary systems fail. Procedures will be tested to verify that the documented steps are accurate and easy to follow, as well as to ensure that the alternative system operate as intended.

Appendix A: District Information Systems

Information System	Type of Information Stored	Type of System	Stakeholders
Network directories and services	Active Directory, DHCP, DNS, NPS, network monitoring and troubleshooting	Premise	All employees Students Community
Google GSuite for Education	Email, Scheduling, District files, Google directory	Cloud	All employees Students Community
Internet and Wifi Access	Wireless, layer 2 and 3 network configurations	Premise network hardware	All employees Students Community
DAN5 Windows file server	District files	Premise	District Office employees, site administrators
Q Student Information Systems	Student records	Premise	Teachers, site administrators, site counselors and other support service providers, district tech/fiscal/HR staff. Parent/guardians Students
Escape	Financial and Employee records	Cloud (Private: ACOE)	Site administrators, fiscal and HR staff
Nutrikids	Nutrition and food services records	Premise	Child Nutrition Services staff

Information System	Type of Information Stored	Type of System	Stakeholders
Destiny	Library & instructional resource records	Premise	Media Services staff; Tech Services staff
Clever Learning Management System / Instructional Portals	Tynker, Matific, Benchmark	Cloud	Teachers, site administrators Students
Miscellaneous Learning Management Systems & Instructional Portals	McGraw Hill, Naviance, Pearson, Illuminate, Moodle (premise), SWIS,	Cloud	Teachers, site administrators Students
BMET	Bond accounting and project management	Cloud	Facilities and fiscal staff
Disc Image	Electronic document retention and management	Premise	District Office staff
Miscellaneous Operational Portals	Aesop, Facilitron, School Dude, Digital Reel, Escape Employee Portal, Blackboard, Agenda Online, RT Technology Workorders (premise)	Cloud	All employees
Telephone and voice mail servers	Landline telephone services	Premise	All employees Community

Appendix B:

Summary of Planned Network and Data Resiliency Improvements

Activity	Anticipated Timeline	Estimated Costs	Proposed Funding Source
Install disaster recovery redundant servers (hot site) (phase 1)	2019-20	$300 K (one-time)	Measure I1
Install disaster recovery site redundant network infrastructure (phase 2)	2020-21	$150K (one-time)	Measure I1
Install disaster recovery redundant internet service (phase 2)	2020-21	$50K (annual recurring)	General Fund; e-Rate
Upgrade data backup systems (cold storage): premise system	2019-20	$50K (one-time)	Measure I1
Upgrade data backup systems: cloud system	2019-20	$6K (annual recurring)	General Fund
Install District Office data center backup power solutions	TBD	TBD	TBD
Install disaster recovery site backup power solutions	TBD	TBD	TBD
Implement VOIP telecommunications infrastructure for landline and mobile phones, voicemail and campus communications (including emergency communications systems)	Life of plan	$6M (one-time)	Measure I1
Implement VOIP external telephone services	2020-21	$150K (annual recurring)	General Fund