Mt. San Antonio College - DRP Summary

Document Information

Security Level:	Internal Use only – Yellow	Version #:	1.1
Author:	Chris Schroeder	Version Date:	8/12/2022
Owner/Approver:		Document Status:	
Version History and Comments:	• Updated RTO		

Contents

1 Introduction

A disaster recovery plan (DRP) is a collection of documents and information that outlines how an organization will recover from an IT service disruption. This document is a summary of our organization's DRP components, from analysis to recovery procedures, and overall DR strategy.

Specifically, this document is organized into the following categories:

- **DR requirements:** This includes a summary of scope, business impact analysis (BIA), and risk assessment.
- **DR strategy:** This includes a summary of our recovery procedures, DR site, and backup strategy.
- **Testing and maintenance:** This includes a summary of our DRP testing and maintenance strategy.

1.1 Disaster Recovery Defined

Our DRP establishes the procedures for properly recovering from a disaster affecting IT services. An IT disaster is defined as a service interruption requiring IT to rebuild a service, restore from backups, or activate redundancy at the backup site.

Disasters may arise from a range of incidents, from isolated hardware/software failure of critical systems to more-destructive events such as a fire or flood that impacts much of the data center. Recovery can include:

- **Recovery-in-place.** For example, activating a standby system in the primary data center (e.g. making the secondary server in a cluster the primary server), or repairing the affected system (e.g. replacing failed hard drives in a SAN).
- **Failover to our DR site.** This action could be initiated if there is significant damage to the primary data center facility, or multiple systems in the primary data center, that makes recovery-in-place impractical because RTOs would not be met.

A disaster can also arise from failure of service providers (e.g. WAN, internet, electricity), in which case IT invokes backup providers or restores services at a site unaffected by the outage.

A successful disaster recovery is completed when:

- The affected IT services are restored to end-user functionality within the recovery time objective (RTO).
- The affected data is restored to a point no older than the restore point objective (RPO).
- The end users affected by the outage have access to restored functionality and have been informed as to the recovery status.
- The business and IT agree that the IT services have been restored.

1.2 Scope

1.2.1 In-Scope

Our DRP applies to:

- Our primary data center (1100 Grand Ave, Walnut CA 91789)
- Outsourced services (e.g. cloud-based services)
- Internet access

  Note: The specific hardware and software assets required for our IT services (including servers and other assets required at our DR site to facilitate recovery), as well as system configuration and technical specifications, are captured in our asset management documentation (see section **2.2 Asset Management**).

1.2.2 Out-of-Scope

A DRP is focused on recovery of core IT services. **Business continuity** and **corporate crisis management** needs to be outlined in separate plans.

For example, our DRP does not include:

- Recovery of end-user workstations and devices (or manual workarounds).
- Alternate end-user facilities (if the primary facility can't be occupied).
- Coordinating business continuity plans to invoke manual workarounds (i.e. downtime procedures).
- Coordinating emergency response plans such as evacuation procedures in the event of a fire.

2 DR Requirements

Our DRP is grounded in an analysis of:

- Business impact.
- Assets required for recovery.
- Risk assessment.

2.1 Business Impact Analysis (BIA) Results

A business impact analysis (BIA) has been completed to determine the criticality, recovery time objectives (RTOs), and recovery point objectives (RPOs) of IT services (applications and systems). The BIA has been reviewed and approved by IT and business stakeholders.

This section provides a summary of the BIA results. For more details, refer to the ***DRP Business Impact Analysis*** spreadsheet.

2.1.1 Impact of Downtime Criteria

Immediate financial impact was determined to be fairly low, so the focus of the BIA was on goodwill impact.

Goodwill impact includes the frustration, reputational damage, and general dissatisfaction experienced by customers and staff due to downtime. Customers include donors, beneficiaries, and investment clients. Below is a summary of the goodwill categories that were assessed and examples of impact due to IT downtime:

- **Impact on Students and the Community:** Beneficiaries include the College, its students, and the community. Examples of impact include delays in grading, student transcripts, and financial aid disbursements (urgent requests could be due to the same disaster impacting Mt. San Antonio College.).
- **Impact on Staff:** Examples of impact include staff frustration due to inability to complete their work or the need for manual workarounds.

2.1.2 Tier 1, 2, and 3 Systems (Applications and Infrastructure)

The BIA was used to prioritize applications into three tiers, where Tier 1 is the highest priority. Below is a summary list of Tier 1, 2, and 3 applications.

2.1.2.1 Tier 1 (mission critical)

- Core Infrastructure
- Banner
- Luminis
- OnBase
- Ethos Identity Manager
- Email (Office 365 for staff, Google for students)
- Phone system
- Life and Safety Systems (Alertus, RAVE)

2.1.2.2 Tier 2

- File servers (unstructured data)
- Classrooms (including lab computers)
- Audio/Visual systems
- SARS/SARSGrid

2.1.2.3 Tier 3

- Print Servers
- Security Cameras

*[**Note:** Additional systems are outside the scope of this example, and have been redacted.]*

2.1.3 Targets for Acceptable Downtime and Data Loss

2.1.3.1 RTO and RPO Definitions

- **Recovery time objective (RTO) – i.e. acceptable downtime target:** This is the target for the maximum amount of time to recover IT systems.
- **Recovery point objective (RPO) – i.e. acceptable data loss target:** This is the target for the maximum amount of data loss due to an IT incident (e.g. if it's necessary to restore data from backups).

2.1.3.2 RTA and RPA Definitions

- **Recovery time actual (RTA) – i.e. potential maximum downtime:** This is an estimate of how long it could take to recover IT systems.
- **Recovery point actual (RPA) – i.e. potential maximum data loss:** This is an estimate of how much data loss in hours could result from an IT incident (e.g. if it's necessary to restore data from backups).

2.1.3.3 RTO/RPO and RTA/RPA Summary

These values are based on a full data center failure (i.e. failover to the DR site is required). RTAs/RPAs can be shorter for more-isolated events.

	Maximum Downtime		**Maximum Data Loss**	
Criticality	**RTO (hh:mm)**	**RTA (hh:mm)**	**RPO (hh:mm)**	**RPA (hh:mm)**
Tier 1	24:00	**24:00**	*0-24:00	***0-24:00**
Tier 2	24:00-48:00	**24:00**	24:00	**24:00**
Tier 3	48:00-168:00	**48:00**	24:00	**24:00**

***Note:** RPO for most systems is 24 hours. The exceptions are:

- **Email (RPO and RPA is zero):** Office 365 is used for staff email. Google is used for student email.

2.2 Asset Management and System Configuration Details

2.2.1 Asset Management

Hardware and software asset details are maintained in our asset management tool, Lansweeper. Tracked details include:

- Hardware specifications
- Software version
- Licensing details

Assets are tracked in Lansweeper through their lifecycle, from procurement to decommissioning. Relevant details are exported monthly to Excel spreadsheets maintained in our DRP repository for reference purposes.

2.2.2 System Configuration Details

System configuration details are maintained in our system documentation and change logs. Tracked details include:

- Hardware/software configuration.
- A history of changes in hardware/software configuration.

System configuration details are documented as part of our release control and change management procedures.

2.2.3 Relevance to DR

Asset management and software configuration details provide the information necessary to:

- Rebuild systems if required (e.g. specs to procure appropriate hardware, and required system configuration details).
- Identify appropriate systems for our DR site to provide adequate performance and capacity.

2.3 Risk Assessment

Our primary data center is located in an area where severe natural disasters are rare. In addition, we recognize that the more likely risks of downtime would be power outages, network outages, hardware, and software issues. With the above in mind, the following mitigation strategies are in place:

Risk	**Mitigation**
Widespread destructive event (e.g. earthquake, tornados) that causes an outage at the primary and DR site.	Offsite backups in AWS would enable recovery in the unlikely event that the primary and DR sites are both severely damaged. Recovery would be much longer than acceptable RTOs, and this risk is accepted by the Board of Directors.
Fire	A DR site is required to enable recovery within acceptable RTOs/RPOs (does not currently exist).
Flood	
Hazardous spill or similar event that prevents access and potentially requires power shutoff (e.g. due to a gas leak).	
Power outage	Uninterruptible Power Supply with standby generator.
Network outage	Network redundancy (e.g. secondary Internet connection). If necessary, can also failover to the DR site within acceptable RTOs/RPOs.
System failure (hardware or software)	Most critical systems have redundancy (e.g. core switch cluster, with auto-failover, resulting in negligible downtime).

Note: Additional risk assessment details are available from our Corporate Risk Management team.

3 DR Strategy

This section summarizes our DR solution (i.e. our DR site and backup strategy) and recovery procedures.

3.1 DR Site

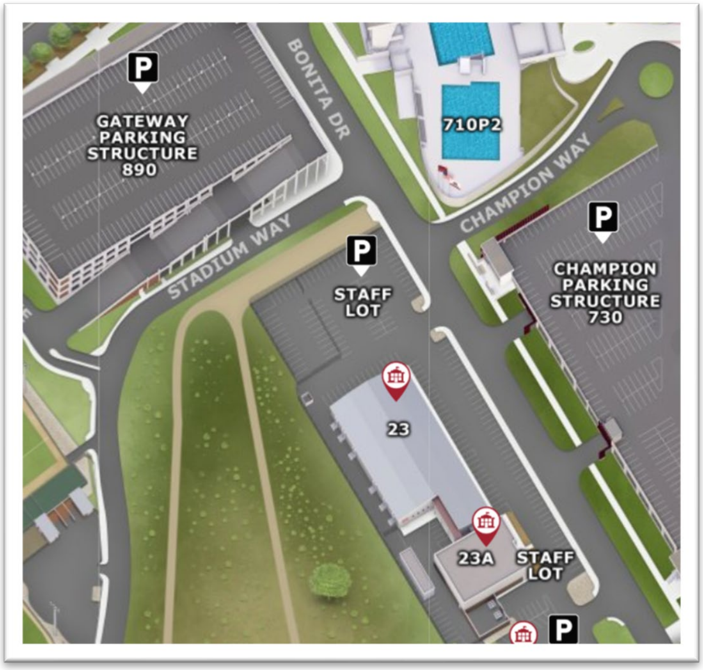
3.1.1 Facility Overview

- The College does not currently have a DR or alternate processing site.

3.1.2 Map View of Our Primary and DR Site Locations

- The College does not currently have a DR or alternate processing site.

Map of Primary Site for building 23A



Map of DR Site

n/a

3.1.3 DR Site Provisioning

The College does not currently have a DR or alternate processing site.

- *The College does not currently have a DR or alternate processing site.*

Regarding compute capacity:

- If the primary data center fails… The College does not currently have a DR or alternate processing site.

For more details, see section **2.2 Asset Management and System Configuration Details.**

3.2 Backup Strategy

3.2.1 Primary Backups

Data is replicated between the primary and DR site at frequencies that reflect system criticality (e.g. critical databases are replicated in near-real time).

In addition, data is backed up nightly from our primary data center to our DR site and meets the requirements for our acceptable RPOs:

Application Tier	**RPO (hh:mm)**	**Backup Frequency (hh:mm)**
Tier 1	24:00	24:00
Tier 2	24:00	24:00
Tier 3	24:00	24:00

Note: For more details, see “RTO/RPO and RTA/RPA Summary.”

3.2.2 Offsite Backups

As noted above, backups are stored in AWS in US West-2.

3.3 DR Incident Response Plan

3.3.1 Overview

The DR incident response plan consists of the following documentation:

Recovery Workflow:

- High-level incident response plan in flowchart format. This provides a recovery roadmap for the overall DR team and is especially useful to the DR Team Leader who needs an at-a-glance view of the overall plan to coordinate incident response.
- Includes assessment and initial response (e.g. initial detection/notification, assessment, and disaster declaration) as well as system recovery workflows.

Notification, Assessment, and Disaster Declaration Procedures,
and the **Recovery Playbook:**

- More-detailed procedures that expand on the steps outlined in the Recovery Workflow.
- Includes links to relevant supporting documentation (e.g. configuration documents, vendor manuals).

Supporting Documentation:

- Documentation that supports day-to-day infrastructure management (e.g. asset management records, network diagrams, configuration documents) and that may be referenced by the Playbook to support recovery procedures.

  - Also includes governance documentation that may need to be referenced, such as the BIA (recovery priorities) and the Teams & Contacts document (clarifies responsibilities and alternates for key roles).

For details about how DRP documentation is stored, managed, and accessed, see “DRP Documentation Management.”

3.3.2 Assessment and Declaration

Assessment and declaration procedures are included in the Incident Response Plan. The decision to declare a disaster and initiate a failover to our DR site is based on:

- Expected duration based on damage assessment, and whether that exceeds the RTO.
- An evaluation of the time required to failover to our DR site vs. repair-in-place.
- Business impact (e.g. are Tier 1 system(s) down?).

3.3.3 Communications During a Disaster

Notification and communication procedures (e.g. escalation path for potential DR incidents, as well as guidelines for communicating status to business users) are outlined in the Incident Response Plan.

In addition:

- Each member of the DR team maintains contact information on their cell phones for all members of the DR team.
- A full list of the crisis management team and DR team, as well as key vendor contacts, are maintained in the ***DRP Teams and Contacts*** document**.**

3.4 Procedures for IT Operations While in DR Mode

3.4.1 While Executing DR Procedures

IT operations will be managed as follows:

- The priority for all IT staff will be to support DR procedures. All other tasks will be put on hold as needed.
- Communications to all staff and students with status updates are expected to reduce, but not eliminate, calls to the Service Desk. In addition:
  - The Helpdesk Desk team will revise the standard greeting to refer to DR status updates.
  - Submitted tickets will not be escalated until IT staff have been released from DR obligations.

3.4.2 After Failover to the DR Site Is Completed

The procedures for most standard IT operations will not change, with the exception that more tasks will be done remotely (most of the IT staff is based at the primary data center).This includes normal system administration, Service Desk procedures, and incident management.

Data replication and backup procedures will follow a different process:

- Backup procedures are put on hold during the first 24 hours of recovery.
- After 24 hours, the DR team will resume offsite backups (to AWS).

3.5 DR Awareness and Training

The Core DR team is responsible for supervising and ensuring that the entire DR team is aware and trained to execute the relevant DR procedures. DR awareness and training includes:

- Annual review of roles and responsibilities.
- Annual review of DR documentation.
- Introduction to the above content during new employee onboarding procedures.
- A series of DR tests each year (see “DR Testing”).

3.5.1 Roles and Responsibilities

The roles and responsibilities for the DR team are outlined in the DRP Workbook, reviewed as part of an annual DRP review, and reviewed as part of DR testing.

The following is a summary of what is outlined for each team member:

- Specific role (e.g. DR Team Leader, system recovery role, and communication role).
- Alternates for each role.
- Specific responsibilities, such as system recovery responsibilities.
- Authority to declare a disaster (this applies to the DR Team Leader and alternate).
- Spending authority during a disaster.

For more details, refer to the ***DRP Reference Workbook.***

4 Testing and Maintenance

A structured program is outlined to review, maintain, and optimize the DRP through:

- DR testing.
- Documentation management (including formal reviews).
- Change management.

4.1 DR Testing

Our annual testing program includes:

- Tabletop planning exercises in Q1 and Q2. This enables the DR team to ensure procedures are current and resolve issues before more functional testing in Q3 and Q4.
- Simulation testing in Q3 (i.e. activate systems at the DR site in a controlled manner to verify system functionality).
- Parallel testing in Q4 (i.e. repeat the simulation testing, but add the execution of UAT scripts with business users to validate system integrations and appropriate report outputs).

Each test includes a record of issues found and action items to resolve those issues before the next test. This drives ongoing DR awareness, DRP accuracy, and successful follow-up testing.

For more details, refer to our DR test plans.

4.2 DRP Documentation Management

Everyone on the DR team will be responsible for contributing to DR documentation and following our standard documentation management guidelines to ensure consistency. DRP reviews include ensuring that proper document management procedures are followed.

DRP documentation is maintained in the following locations:

- **Primary DRP Repository:** Microsoft Teams – (https://mtsac0.sharepoint.com/:f:/s/IT-Network&InfoSec/ErBByPsZJIBFhZzrb96jBFkB2Cm6G32YCHjyJ5z-ykoMtg?e=xUy8e0)
- **Primary Backup:** Stored on the smartphones of all DR team members (see the DRP Reference Workbook). Team members receive monthly notifications to download an updated copy.
- **Secondary Backup:** A full copy of all DR documentation is printed once per year and kept in a locked office at the DR site.

4.3 DRP Change Management

4.3.1 Day-to-Day Change Management

DR considerations are incorporated into our change management process to ensure that changes in the business and technology environment are consistently reflected in our DRP.

This includes the following process points:

- Asset management records are updated as assets are added or decommissioned. In addition, asset management records are audited annually. Our DRP leverages the asset management information directly (rather than making a copy) so our asset management references in our DRP are kept up to date by default.
- New IT projects include an outline of DR requirements:
  - Requirements gathering for new applications includes determining RTOs/RPOs based on impact of downtime and technical requirements to meet those targets.
  - Similarly, proposed changes to our IT environment requires an outline of potential impact on DR capability, and changes to DR requirements.
  - DR requirements are noted as project requirements, and therefore, monitored through the existing project checkpoints, with the assistance of the DRP Coordinator.
- Change management for business operations also includes a summary of how the change affects business impact and RTOs/RPOs. For example, introduction of new services includes an assessment of whether those services require a change in RTO/RPO for relevant applications. The DRP Coordinator will manage how changes are incorporated into our DRP.

4.3.2 DRP Annual Review

Our DRP is reviewed annually to:

- Validate that required updates identified through testing and change management have been incorporated in the DRP.
- Provide a focused review of elements of the DRP that have undergone significant change.

5 Summary

Service continuity, and therefore our DRP, is a high priority for our organization. Our organization is committed to maintaining an effective DRP that includes:

- Clearly defined DR requirements through a business impact analysis.
- Ongoing evaluation of our DR strategy and DR capabilities to reduce RTO and RPO values where they exceed acceptable values.
- Rigorous DR change management practices to ensure our DRP stays current.