DISASTER RECOVERY PLAN

1.0 Plan Introduction

Monterey Peninsula College(MPC) recognizing their operational dependency on computer systems, including the Local Area Network (LAN), Database Servers, Internet, Intranet and e-Mail, and the potential loss of revenue and operational control that may occur in the event of a disaster; authorized the preparation, implementation and maintenance of a comprehensive IT disaster recovery plan.

The intent of a Disaster Recovery Plan (DRP) is to provide a written and tested plan directing the computer system recovery process in the event of an interruption in continuous service resulting from an unplanned and unexpected disaster. The DRP is a working document and will be periodically updated as enhancement are made.

The Disaster Recovery Plan preparation process includes several major steps as follows:

- Identify systems and applications currently in use
- Analyze business impact and determine critical recovery time frames
- Determine recovery strategy
- Document recovery team organization
- Document recovery team responsibilities
- Develop and document disaster recovery procedures and checklists

These steps were conducted and this document represents the completed effort in the preparation of the MPC IT Disaster Recovery Plan.

1.1 Mission and Objectives

The mission of the IT Disaster Recovery Plan is to establish defined responsibilities, actions, and procedures to recover the MPC computer, communication, and network environment in the event of an unexpected and unscheduled interruption. The plan is structured to attain the following objectives:

- Recover the physical network
- Recover the applications
- Minimize the impact on the college with respect to operational interference

1.2 Disaster Recovery / Business Continuity Scope

The scope of the plan is to recover computer information services provided by the MPC Datacenter located on the main campus, first floor of the Administration Building, 980 Fremont Street, Monterey Ca. The network encompasses the following:

- Critical business applications such as Student Information Systems (SIS)
- File servers supporting all business operations
- Gateway to the host applications and other sites
- Wired and wireless networks
- Campus phone system

1.3 Responsibility

The responsibility for ensuring the plan is maintained and tested rests with the MPC Information Technology Department under the leadership of the Director of Information Services / Chief Information Systems Officer (CISO). This plan will be updated and presented to Technology Committee periodically. The updated DRP will be an appendix to the 2016 – 2019 Technology Plan.

2.0 Business Impact Analysis

The Business Impact Analysis is completed to determine the Critical Time Frame in which the application system capabilities and functionality must be available after an interruption in service to minimize the operational loss of control and potential loss of revenue. In addition, the Business Impact Analysis assists in identifying alternative manual procedures which may be used during an interruption in service. Therefore, the objectives of the Business Impact Analysis are:

- Educate user on the need for a disaster recovery plan
- Identify alternative manual procedures which may temporarily minimize impact due to an interruption in computer service

It is considered best practice to conduct a business impact analysis for each physical location, application, business function, department, and organizational entity annually. In addition, as conditions change (i.e. event like 9/11) to alter the operating environment, at least the risk component should be reviewed and actions taken to mitigate un-acceptable levels of risk.

Legend of Impact Score

1 = Catastrophic – as a result MPC could cease to exist and/or would be placed in material legal and/or financial jeopardy.
2 = Very High - as a result MPC would not be able to meet its material contractual and/or service obligations. Or do material damage to MPC's reputation and have major negative long term implications on MPC's ability to continue being a going concern.
3 = Noticeable - MPC would not be able to operate effectively and efficiently, thus reducing productivity and service levels.
4 = Minor – MPC would be affected in a minor way with little productivity and/or service level loss.
5 = Non-essential – MPC could operate indefinitely without this physical location, business function, or IT application.

2.1 Application/Systems Inventory and Risk Scores

A summary of the major business systems and their impact scores are shown below.

Locally Hosted Systems

SIS servers and storage - Impact score 1

File Servers / Storage – Impact score 1 to 2

EMS – Impact Score 2

Powerfaids – Impact Score 2

DNS, DHCP – Impact Score 1

Cloud Hosted Systems

Webpage – Impact score 2

Single Sign-On – Impact score 2

Email – Impact score 1

.

3.0 Backup & Restore Strategy

The MPC IT department maintains a Data Center with Uninterruptible Power Supplies (UPS) that provides one hour emergency power to the servers as well as adequate cooling/humidity control systems for all its critical systems including servers and network equipment. The Data Center is connected to a gas powered generator that starts when power to the campus is lost. Spare, preconfigured network switches are available to be deployed in the case of hardware failures. All servers are backed up daily from Monday through Friday and monitored to ensure timely recovery from a system failure, system crash or natural disaster.

In the event of a disaster, the disaster recovery team would be assembled and a plan of restoration would be put in place. The systems would be prioritized (see section 2.1) and restored accordingly.

Information technology systems require hardware, software, data and connectivity. Without one component of the "system," the system may not run. Therefore, specific recovery strategies will anticipate the loss of one or more of the following system components:

- Data Center environment (secure computer room with climate control, conditioned and backup power supply, etc.)
- Hardware (networks, servers, desktop and laptop computers, wireless devices and peripherals)
- Connectivity to network (fiber, cable, wireless, etc.)
- Software applications (electronic data interchange, electronic mail, enterprise resource management, office productivity, etc.)
- Data and restoration

3.1 Data Capture and Backups

Backups performed using System Center 2012 SP1 Data Protection Manager
Short term backups are to disk, long term backups are to Virtual Tape Drives using HP StoreOnce 4220 Backup solution with deduplication
Other than Bare Metal Backups, long term backups are kept for 1 year

☐ Bare Metal Backups of all Domain Controllers- short term weekly, long term every 2 weeks

☐ Bare Metal Backups for other mission critical servers - short term weekly, long term monthly retained for 2 months

☐ All user data and shares –short term every 12 hours, retained for 14 days and weekly retained for 2 weeks– long term monthly backups are retained for 1 year

☐ SharePoint Websites –short term daily, retained for 2 weeks– long term monthly backups are retained for 1 year

☐ Student Records System –short term every 15 minutes, retained for 7 days- long term weekly retained for 1 month, monthly retained for 1 year

☐ All SQL Databases – short term every 6 hours, retained for 2 weeks – long term every 2 weeks then monthly retained for 1 year

- All network equipment configuration is backed up nightly

3.2 Preventative Measures

Following are several preventative measures that, when implemented and monitored on a regular basis will reduce the chance of a computer disaster ever occurring or minimize its impact.

- Restrict access to the Data Center to authorized personnel only
- Ensure there are no combustible materials located in the Data Center, such as solvents, paper, etc.
- Conduct regularly scheduled service on support systems, such as the Air Conditioning, Fire Retardant and UPS systems
- Check for overloaded circuits or worn/damaged electrical and power cables
- Perform regularly scheduled backups

4.1 Data Recovery

4.1.1 Recovery Management Team

The Recovery Management Team is responsible for managing the recovery effort as a whole, ensuring restoration occurs within planned Critical Time Frames and assists in resolving problems requiring management action. The Recovery Management Team consists of the Director of Information Services, Network Engineers and Network Technicians. The team is activated at the call of the Director of Information Services when a disaster occurs. Specifically, the Recovery Management Team is charged with:

Pre-Disaster

- Approves the final Disaster Recovery Plan
- Ensures the Disaster Recovery Plan is maintained
- Ensures Disaster Recovery training is conducted
- Authorizes periodic Disaster Recovery Plan testing
- Maintains and updates the plan as scheduled
- Distributes Disaster Recovery Plan to recovery team members
- Appoints recovery team members and alternates as required
- Coordinate the testing of the plan
- Trains disaster recovery team members in regard to the Plan

Post-Disaster

- Declares that a disaster has occurred and the Disaster Recovery Plan is activated
- Determines the plan strategy to be implemented
- Determines alternate team members (if any) and other support members of the recovery process
- Manages and monitors the overall recovery process
- Advises Senior MPC and user management on the status of the disaster recovery efforts

5.0 Future Enhancements

Following are several future enhancement that will improve the robustness of the backup and recovery process:

- Identical backup solution configured at the Marina Education Center
- Cloud backups for all appropriate systems and data
- Reduction of local physical servers and storage, utilizing virtualization and cloud hosting.
- Expanding Uninterrupted Power Supplies (UPS) to provide power backup to critical systems locally throughout the campuses
- Cloud based Active Directory (AD) as redundancy for local AD.
- Develop and test disaster recovery scenarios.
- Implement Enterprise Resource Planning (ERP) to consolidate systems.