INFORMATION SECURITY- DISASTER RECOVERY

1.0 Purpose and Scope

The objective of this Administrative Regulation is to outline the strategy and basic procedures to enable Yosemite Community College District (YCCD) to withstand the prolonged unavailability of critical information and systems and provide for the recovery of District Information Technology Services (ITS) services in the event of a disaster.

This is one of a series of information security Administrative Regulations maintained by the District Information Technology Services (ITS) department designed to protect YCCD information systems.

1.1 Applicability of Assets

This Administrative Regulation has been designed and written to be used in the event of a disaster affecting YCCD at the District's central business offices in Modesto, CA.

Disaster Recovery plans are applicable to Tier 1 (critical) information technology components of YCCD. A determination has been made based on an internal risk assessment which business applications are considered to be Tier 1.

1.2 Applicability to all Employees and Volunteers

This Administrative Regulation applies to all Board of Trustees authorized/ratified full-time and part-time regular Academic and Classified employees, Substitutes, Short-term (Temporary) staff, Professional Experts, College Work Study students, Student Help and Volunteers who are employed in the Yosemite Community College District for the purpose of meeting the needs of students.

1.3 Applicability to External Parties

May have applicability to external parties to the extent that hardware, software or services provided by or utilized by the external party is affected by the disaster.

2.0 Disaster Recovery

Disaster Recovery (DR) is best described as the plans and activities designed to recover technical infrastructure and restore critical business applications to an acceptable condition. DR is a component of Business Continuity Planning, which is the process of ensuring that essential business functions continue to operate during and after a disaster.

2.1 Disaster Recovery Strategy and Components

This plan is structured around teams, with each team having a set of specific responsibilities.

The YCCD Disaster Recovery strategy is based on the following elements:

- ITS infrastructure designed with redundancy and application availability in mind
- The ability to leverage cloud-based or alternate site locations and facilities
- Documented and tested ITS Disaster Recovery procedures for each Tier 1 application
- Business Continuity plans as developed by associated business areas

This Administrative Regulation describes:

- Disaster declaration
- A priority list of critical applications and services to be recovered
- Key tasks that include responsibilities and assignments for each task
- Departments and individuals who are part of the recovery process

2.2 Business Continuity Plans

The Disaster Recovery Plan for a critical application is a complementary subset of departmental Business Continuity Plans (BCPs). These plans describe the actions to be taken within business areas that rely upon and use those applications.

Copies of BCPs will be documented and maintained by YCCD business units as led and developed by the relevant Business Recovery Coordinator. The ITS Disaster Recovery Coordinator will retain master copies of all YCCD BCPs.
All relevant YCCD employees must be made aware of the Business Continuity Plan and their own respective roles. Training must be provided to staff with operational business and /or recovery plan execution responsibilities.

Business Continuity Plans must be developed with requirements based on the specific risks associated with the process or system. Business Continuity Plans must include, but are not limited to, the following information:

1. Executive Summary
2. Key Assumptions
3. Identified Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO)
4. Long-term vs. Short-term Outage Considerations
5. Disaster Declaration / Plan Activation Procedures (e.g., communication plan, mobilization plan)
6. Key Contacts / Calling Tree(s)

7. Roles / Responsibilities (e.g., Recovery Teams)
8. Alternate Site / Lodging
9. Asset Inventory
10. Detailed Recovery Procedures
11. Relevant Disaster Recovery Plan
12. Event and recover status reporting to YCCD management, appropriate employees, third parties and business partners.

Sufficient detail must be included so that procedures can be carried out by individuals who do not normally perform these responsibilities.

2.3 Roles and Responsibilities

2.3.1 Disaster Management Team

The Disaster Management Team is responsible for providing overall direction of the data center recovery operations. It ascertains the extent of the damage and activates the recovery organization. Its prime role is to monitor and direct the recovery effort. It has a dual structure in that its members include Team Leaders of other teams. Responsibilities of the Disaster Management Team include:

- Evaluating the extent of the problem and potential consequences and initiating disaster recovery procedures
- Monitoring recovery operations; managing the Recovery teams and liaising with YCCD management and users as appropriate; notifying senior management of the disaster, recovery progress and problems
- Controlling and recording emergency costs and expenditures; expediting authorization of expenditures by other teams
- Approving the results of audit tests on the applications which are processed at the standby facility shortly after they have been produced
- Declaring that the Disaster Recovery Plan is no longer in effect when critical business systems and application processing are restored at the primary site

The Disaster Management Team Leader is responsible for deciding whether or not the situation warrants the introduction of disaster recovery procedures. If he/she decides that it does, then the organization defined in this section comes into force and, for the duration of the disaster, supersedes any current management structures.

The Disaster Management Team will operate from a Command Center (TBD), or, if that is not possible, at a secondary location TBD.

The team members are:

Title / Department
Assistant Vice Chancellor, Technology
Director of Enterprise Services – Enterprise Operations
Director of Enterprise Services – Systems Development and Programming and Help Desk
Director of Enterprise Services – Technology Regulations, Procedures and Guidelines Development

2.3.2 Recovery Coordinators

There are two coordination roles who will report to the Disaster Management Team:

- A Disaster Recovery Coordinator (*to be appointed*) is the communications focal point for the Disaster Management Team and other Teams, and will coordinate disaster notification, damage control, and problem correction services. The Disaster Recovery Coordinator also maintains the IT Disaster Recovery Plans and offsite copies, and retains master copies of Business Recovery Plans.

- Business Recovery Coordinator (*to be appointed*) will be the focal point for Business Recovery. Assists Colleges and District offices development and maintenance of their Business Recovery Plans and coordinate recovery efforts and notification in the business areas.

2.3.3 Operations Team

The Operations Team is responsible for the computer environment (Data Center and other vital computer locations) and for performing tasks within those environments. This Team is responsible for restoring computer processing and for performing Data Center activities, including:

- Installing the computer hardware and setting up the latest version of the operating system at the standby facility.
- Arranging for acquisition and/or availability of necessary computer equipment and supplies
- Establishing processing schedule and inform user contacts
- Obtaining all appropriate historical/current data from the offsite storage vendor
- Restoring the most current application systems, software libraries and database environments.
- Coordinating the user groups to aid the recovery of any non-recoverable (i.e., not available on the latest backup) data
- Providing the appropriate management and staffing for the standby data center and backup library in order to meet the defined level of user requirements.

- Performing backup activities at the standby site.
- Providing ongoing technical support at the standby site.
- Working with the Networks Team to restore local and wide area data communications services to meet the minimum processing requirements.
- Ensuring that all documentation for standards, operations, vital records maintenance, application programs etc. are stored in a secure/safe environment and reassembled at the standby facilities, as appropriate.

2.3.4 Network Team

The Network Team is responsible for all computer networking and communications, to include:

- Evaluating the extent of damage to the voice and data network
- Discussing alternate communications arrangements with telecom service providers, and ordering the voice/data communications services and equipment as required
- Arranging new local and wide area data communications facilities and a communications network that links the standby facility to the critical users
- Establishing the network at the standby site, and installing a minimum voice network to enable identified critical telephone users to link to the public network
- Defining the priorities for restoring the network in the user areas
- Supervising the line and equipment installation for the new network
- Providing necessary network documentation
- Providing ongoing support of the networks at the standby facility
- Re-establishing networks at the primary site when the post-disaster restoration is complete

2.3.5 Facilities Team

The Facilities Team is responsible for the general environment including buildings, services, and environmental issues outside of the Data Center. This team has responsibility for security, health and safety and for replacement building facilities, including:

- In conjunction with the Disaster Management Team, evaluating the damage and identifying facility equipment which can be salvaged
- Arranging all transport to the standby facility.
- Arranging for all necessary office support services.
- Controlling security at the standby facility and the damaged site. (physical security may need to be increased)
- Working with the Network Team to have lines ready for rapid activation

- As soon as the standby site is occupied, cleaning up the disaster site and securing that site to prevent further damage
- Administering the reconstruction of the original site for recovery and operation
- Supplying information for initiating insurance claims, and ensuring that insurance arrangements are appropriate for the circumstances (i.e., any replacement equipment is immediately covered, etc.)
- Maintaining current configuration schematics of the Data Center (stored off site). This should include:
    - air conditioning
    - power distribution
    - electrical supplies and connections
    - specifications and floor layouts
- Dealing with staff safety and welfare
- Working with Campus police, who will contact local law enforcement if needed

2.3.6 Communications Team

The Communications Team is responsible for obtaining communications directives from the Disaster Management Team, and communicating information during the disaster and restoration phases to employees, suppliers, third parties and students. All information that is to be released must be handled through the Public Information Officer (PIO).

The Communications Team may be made up of the PIO and individuals from Colleges, Marketing, Legal, ITS, HR, and business area organizations, as appropriate.

- Liaising with the PIO, Disaster Recovery Coordinator and/or Business Recovery Coordinators to obtain directives on the messages to communicate
- Making statements to local, national and international media
- Informing suppliers and students of any potential delays
- Informing employees of the recovery progress of the schedules using available communications methods
- Ensuring that there are no miscommunications that could damage the image of the district
- Any other public relations requirements

2.4 Update, Testing and Maintenance

This Disaster Recovery plan must be kept up to date. It is the responsibility of the Disaster Recovery Coordinator to ensure that procedures are in place to keep this plan up to date. If, while using this plan, any information is found to be incorrect, missing or unclear, please inform the Disaster Recovery Coordinator so that it may be corrected. It is important that everyone understands their role as described in this plan.

This Administrative Regulation and the ITS Disaster Recovery Plans must be reviewed by ITS and business management at least semi-annually and when significant application or infrastructure changes are made.

Plans must be tested periodically and at least annually, and include realistic simulations involving the business users and District ITS staff. The results of DR tests must be documented and reviewed and approved by appropriate management.

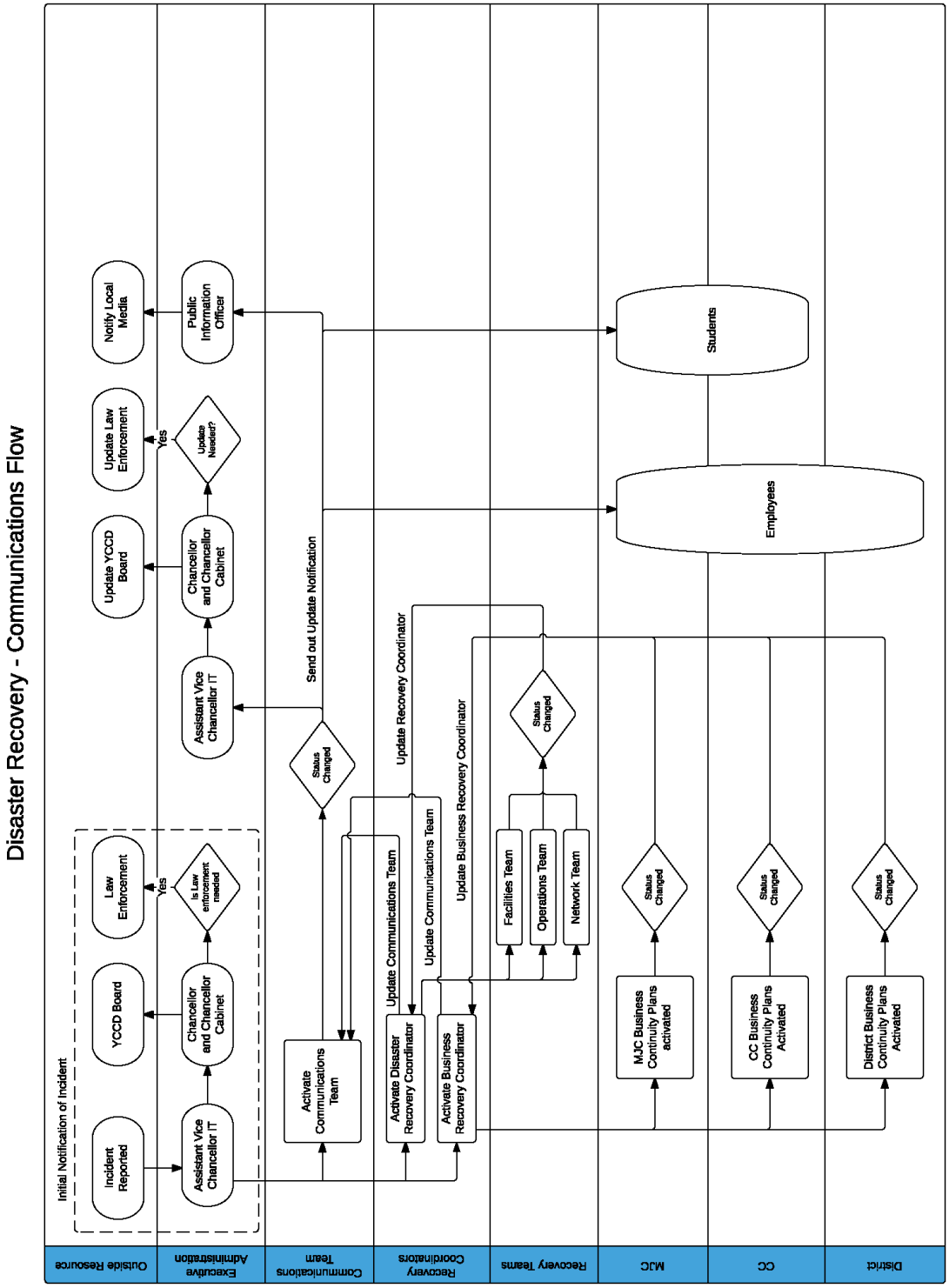
3.0 Communications Plan

The diagram on the next page represents the communication flow in the event of a disaster, Communication flow starts as soon as the disaster is identified or reported.

Regular updates will be made, the interval of the updates will be determined by the severity and duration of the event. Communications will be made utilizing one or more of the following methods depending on service availability.

- Email
- Text message
- Phone
- In person

The Diagram represents communication flow for a worst case event such as the total loss of a datacenter (Level 3 or 4 outage). Shorter term outages may not have all areas and teams activated.


Disaster Recovery - Communications Flow
Initial Notification of Incident
Incident Reported
Assistant Vice Chancellor IT
YCCD Board
Chancellor and Chancellor Cabinet
Law Enforcement
Is Law enforcement needed
Yes
Update YCCD Board
Chancellor and Chancellor Cabinet
Update Needed?
Yes
Update Law Enforcement
Notify Local Media
Public Information Officer
Assistant Vice Chancellor IT
Send out Update Notification
Activate Communications Team
Status Changed
Update Communications Team
Activate Disaster Recovery Coordinator
Update Recovery Coordinator
Activate Business Recovery Coordinator
Update Business Recovery Coordinator
Facilities Team
Operations Team
Network Team
Status Changed
MJC Business Continuity Plans activated
Status Changed
CC Business Continuity Plans Activated
Status Changed
District Business Continuity Plans Activated
Status Changed
Students
Employees
Outside Resource
Executive Administration
Communications Team
Recovery Coordinators
Recovery Teams
MJC
CC
District

4.0 What to do in the Event of a Disaster

The most critical and complex part of disaster response is mobilizing the required personnel in an efficient manner during the invocation of the plan. Because normal processes have been disrupted, individuals are taking on new roles and responsibilities and must adapt to changing circumstances quickly.

The key is for personnel to be well-rehearsed, familiar with the Disaster Recovery Plan, and be sure of their assignments.

4.1 Standard Emergency Plan

The first priority in a disaster situation is to ensure safe evacuation of all personnel.

In the event of a major physical disruption, standard emergency procedures must be followed. This means immediately:

- Activating the standard alarm procedures for that section of the building to ensure that emergency authorities (fire, medical, law enforcement, etc.) are correctly alerted

- If necessary, evacuating the premises following the established evacuation procedures and assemble outside at the designated location, if it is safe to do so.

4.2. First Steps for the Recovery Teams

Action	Team
Evaluate the damage	Disaster Management, Facilities, Operations, Network
Identify the concerned applications	Disaster Management, Operations, Network
Request the appropriate resources for the Standby Facility	Disaster Management
Obtain the appropriate backups	Operations
Restart the appropriate applications at the Standby Facility	Operations
Inform users of the new procedures	Communications
Order replacement equipment to	Operations, Network

replace the damaged computers / networks	
Install replacement equipment and restart the applications	Operations, Network
Inform users of normal operations	Communications

4.3 The Next Steps

- The Disaster Management Team Leader decides whether to declare a disaster and activate the Disaster Recovery Plan, and which recovery scenario will be followed.

- The Recovery Teams then follow the defined recovery activities and act within the responsibilities of each team, as defined in this Disaster Recovery Plan and those defined for the critical applications outlined in the District ITS Business Continuity Departmental Procedures.

4.4 Critical Business Applications / Services

The following business applications are considered critical to YCCD's business:

- Tier 1 application (Ellucian Colleague)
- Tier 1 application (Ellucian CROA)
- Tier 1 application (Microsoft SQL server)
- Tier 1 application (Oracle DBMS)

District ITS departmental procedures shall exist to address the DR procedures for these services.

5.0 Disaster Declaration

In the event of a serious system disruption, the Disaster Management Team will determine the level of response based on the disaster classification categories below. This determination will be made within four (4) hours of the occurrence.

The classification level should be reviewed every 12 hours and re-classification of the disaster will be made as needed until recovery is complete.

Disasters at YCCD fall into one of the following four levels.

Disaster Classification	Description
Level 1 (Low)	**Sub-system Outage / Minor Damage** Partial loss of a component of a critical application for a period of one day to one week. This type of outage does not result in the total loss of operation for that application; however specific functionality is reduced or impaired. In this scenario, only a part of the computer processing environment is impacted, but the communication lines and network are still up and running. The building is still available and the users can use normal office space to wait for the restart of server or application processing. The goal of the recovery process in this case is to restore server or application functionality.
Level 2 (Medium)	**Short Term Outage** Complete loss of a critical application for a period of one day to one week. The ability to meet business functions and mission objectives may be impacted, usually by elongated processing cycles and missed deadlines, but not to a significant extent. In this scenario, a key computer processing application is unavailable. Communication lines or portions of the network may be down. The goal of the recovery process is to restore minimum critical application functionality, which may require moving affected applications to alternate equipment. An alternate site may need to be put on Standby.
Level 3 (High)	**Long Term Outage** Complete loss of a critical application for a period greater than one week but less than two weeks. The ability to continue the business function and its mission is in

Disaster Classification	Description
	jeopardy and may fail in some circumstances, such as missing critical milestones in the business cycle. In this scenario, key portions of the computer processing environment are unavailable. Communication lines or portions of the network may also be down. The goal of the recovery process is to restore minimum critical application functionality either at the primary facility or at the Standby facility.
Level 4 (Critical)	**Total System Disaster** Catastrophic loss of operation of critical system(s) for a period greater than two weeks. Also included in this class are disasters that may not produce outages greater than two weeks, but involve more than one critical application; or natural disasters such as fires, floods, or other catastrophic situations. In this scenario, the entire computer processing environment has experienced a catastrophic disaster and is generally unavailable. Communication lines and/or the network also may not be available. The goal of the recovery process is to restore minimum critical application functionality either at the primary or at the Standby facility as quickly as possible. If time frames for repairs are not acceptable (e.g., will take longer than 1-2 months), an interim or new production facility may need to be acquired or leased.