Status Active PolicyStat ID 17258816

| | |
|---|---|
| Origination | 12/2024 |
| Last Approved | 12/2024 |
| Effective | 12/2024 |
| Last Revised | 12/2024 |
| Next Review | 12/2034 |

| | |
|---|---|
| Chapter Lead | Nohemy Ornelas: Chapter 3(CC),4&5 |
| Policy Area | Chapter 3 General Institution |
| References | Non CCLC |

# AP 3735 Information Security Disaster Recovery



1. PURPOSE AND SCOPE

The objective of this Administrative Procedure is to outline the strategy and basic procedures to enable the District to withstand the prolonged unavailability of critical information and systems and provide for the recovery of District Information Technology (IT) services in the event of a disaster.

This is one of a series of information security Administrative Procedures designed to protect District information systems. The District Information Technology (IT) department has a district-wide fiduciary responsibility to set, maintain, and ensure the provisions of this regulation. District IT accomplishes this through collaborative engagement with the campus Technology Services departments.

a. Applicability

This Administrative Procedure applies to all full-time and part-time regular academic and classified employees, such as short-term (temporary) staff, substitutes, professional experts, Federal Work Study students, and student help, who are employed by, and volunteers who assist the District for the purpose of meeting the needs of students.

b. Applicability to External Parties

This Administrative Procedure applies to all external parties, including but not limited to District business partners, vendors, suppliers, service providers, and other third-party entities with access to District networks and system resources.

c. References and Related Documents

Please refer to the Information Security Administrative Procedures for additional information, references, and definitions.

2. 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.

a. Disaster Recovery Strategy and Components

This plan is structured around teams, with each team having a set of specific responsibilities. The District Disaster Recovery strategy is based on the following elements:

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

This Administrative Procedure describes:

- Disaster declaration.
- A priority list of critical applications and services to be recovered.
- Key tasks that include responsibilities and assignments for each task.

Each critical application that has been identified in this Administrative Procedure has its own Disaster Recovery Plan that can be found in Departmental Procedures.This Administrative Procedure describes:

Paper copies of this Administrative Procedure and Appendices must be stored at secure and readily accessible off-site locations.

b. 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 District business units as led and developed by management. The IT Disaster Recovery Coordinator will retain master copies of all District BCPs (see Section II.C.2 for the description of roles).

Copies of all BCPs must be kept off-site. All plans must be reviewed at least annually and updated for any significant changes.

All relevant District 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:

i. Executive Summary
ii. Key Assumptions
iii. Identified Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO)
iv. Long-term vs. Short-term Outage Considerations
v. Disaster Declaration / Plan Activation Procedures (e.g., communication plan, mobilization plan)
vi. Key Contacts / Calling Tree(s)

vii. Roles / Responsibilities (e.g., Recovery Teams)

viii. Alternate Site / Lodging

ix. Asset Inventory

x. Detailed Recovery Procedures, including the priority order of system recovery

xi. Relevant Disaster Recovery Plan

xii. Event and recovery status reporting to District 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.

c. Roles and Responsibilities

i. 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 District 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 they decide 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 or, if that is not possible, at a secondary location to be determined. The team members are:

- Vice Chancellor of Educational & Student Support Services
- Chief of Technology
- Director of Technical Services

ii. 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 Coordinators (to be appointed) will develop and maintain Business Recovery Plans and coordinate recovery efforts and notification in their business areas

iii. 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 informing 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, help desk, 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 Network 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.

iv. 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.

v. 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 of building facilities, including:

- In conjunction with the Disaster Management Team, evaluate the damage and identify equipment that 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, clean up the disaster site and secure 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.

vi. 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 is made up of the PIO and individuals from colleges, marketing, legal, HR, and business area organizations, as appropriate. This team has the responsibility for:

- 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 communication methods.
- Ensuring that there is no miscommunications that could damage the image of the District.
- Any other public relations requirements.

d. 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.

Updated versions of the plan are distributed to the authorized recipients, listed in Section II.E.

The IT Disaster Recovery Plans, as documented in the Appendices, must be reviewed by IT 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 IT staff. The results of DR tests must be documented, reviewed, and approved by appropriate management.

e. Distribution List

The Disaster Recovery Coordinator is responsible for distributing this plan. Each plan holder, listed in the table below, receives two copies of this plan. One copy is to be kept at the place of work and the other copy at home or other safe and secure offsite location. These copies have an official copy number.

| NAME | COPY NUMBER | LOCATI |
|---|---|---|
| Vice Chancellor, Educational & Student Support Services | DR001 | Office |
| Chief Technology Officer | DR002 | Office |
| District Director, Technology Services | DR003 | Office |
| Director, Secuirty and User Services | DR004 | Office |
| Director, Administrative Applications | DR005 | Office |
| Business Systems Administrator | DR006 | Office |
| College Director, Technology Services (Crafton) | DR007 | Office |

| NAME | COPY NUMBER | LOCATI |
|---|---|---|
| College Directory Technology Services (Valley) | DR008 | Office |
| Public Information Officer | | |

f. 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.

i. Standard Emergency Plan The priority in a disaster situation is to ensure the 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 assembling outside at the designated location if it is safe to do so.

ii. First Steps for the Recovery Teams

| ACTION | TEAM |
|---|---|
| Evaluate the damage | Disaster Management, Facilit Network |
| Identify the concerned applications | Disaster Management, Operat |
| 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 replace the damaged computers/networks | Operatoins, Network |
| Install replacement equipment and restart the applications | Operatoins, Network |
| Inform users of normal operations | Communications |

iii. 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 IT Business Continuity Departmental Procedures.

iv. Critical Business Applications/Services

The following business applications are considered critical to the District's business:

- Tier 1 application (Student Information System)
- Tier 1 application (Financial System)

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

g. 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 the District fall into one of the following four levels.

| DISASTER CLASSIFICATION | DESCRIPTION |
|---|---|
| Level 1 (Low) | **Sub-system Outage / Minor Damage**<br>Partial loss of a component of a critical application for a period of one day to c<br>This type of outage does not result in the total loss of operation for that applic<br>specific functionality is reduced or impaired.<br>In this scenario, only a part of the computer processing environment is impact<br>communication lines and network are still up and running. The building is still a<br>users can use normal office space to wait for the restart of the server or applic<br>The goal of the recovery process, in this case, is to restore server or applicatio |
| Level 2 (Medium) | **Short Term Outage**<br>Complete loss of a critical application for a period of one day to one week.<br>The ability to meet business functions and mission objectives may be impacte<br>elongated processing cycles and missed deadlines, but not to a significant ext<br>In this scenario, a key computer processing application is unavailable. Commu<br>portions of the network may be down.<br>The goal of the recovery process is to restore minimum critical application fun<br>may require moving affected applications to alternate equipment. An alternate<br>be put on Standby. |
| Level 3 (High) | **Long Term Outage**<br>Complete loss of a critical application for a period greater than one week but le<br>weeks.<br>The ability to continue the business function and its mission is in jeopardy and<br>circumstances, such as missing critical milestones in the business cycle.<br>In this scenario, key portions of the computer processing environment are una<br>Communication lines or portions of the network may also be down. |

| DISASTER CLASSIFICATION | DESCRIPTION |
| --- | --- |
| | The goal of the recovery process is to restore minimum critical application fun the primary facility or at the Standby facility. |
| Level 4 (Critical) | **Total System Disaster**<br>Catastrophic loss of operation of critical system(s) for a period greater than tw<br>Also included in this class are disasters that may not produce outages greater but involve more than one critical application; or natural disasters such as fires catastrophic situations.<br>In this scenario, the entire computer processing environment has experienced disaster and is generally unavailable. Communication lines and/or the network available.<br>The goal of the recovery process is to restore minimum critical application fun the primary or at the Standby facility as quickly as possible. |

## Approval Signatures

| Step Description | Approver | Date |
| --- | --- | --- |
| Approved per Level 2 process in AP 2410 | Kelly Goodrich: PPAC Support | 12/2024 |