Administrative Procedure 7226

IT Disaster Recovery

Responsible Office: Office of Information Technology

PURPOSE

The Superintendent has adopted this Administrative Procedure to develop Information Technology (IT) Disaster Recovery and Business Continuity capabilities to anticipate, prevent, and mitigate the impact of disasters including system outages caused by natural and man-made disasters or computer security incidents in the Washoe County School District (District).

DEFINITIONS

1. "Business Continuity" refers to the organization's ability to maintain essential functions during and after a disaster. It is primarily concerned with modifying business processes during a disaster situation to ensure that critical functions can still be performed.

2. "Business Impact Assessment" refers to a methodology for predicting the consequences of disruption to a business function that the District performs which informs recovery strategies and prioritizes resources in Disaster Recovery Planning.

3. "Critical Asset List" refers to a compilation of information resources that are critical for the District to perform regular operations and meet regulatory or compliance objectives.

4. "Communications Management Plan" refers to the methods that stakeholders are notified by in the event of a Disaster.

5. "IT Disasters" are unexpected events that result in a slowdown, interruption, or failure of an information system or network. Disasters can be caused by natural events (earthquake, floods, wildfires, or earthquakes), equipment or infrastructure failures (power outages), man-made disasters (accidental data erasure), or cyber-attacks.

6. "Disaster Recovery" refers to the process of regaining access and restoring functionality used to support critical technology services and assets that are necessary for business operations immediately following a significant man-made or natural disruption (disaster).

7. "Disaster Recovery Plan" refers to a written plan designed to restore information and systems if a disaster occurs.

PROCEDURE

1. Roles and Responsibilities:

a. System Owner

    i. Responsible for the business function that associated IT asset support;

    ii. Ensures that System Disaster Recovery Plans are put in place; and

    iii. Oversees system-level DR Plan testing and validation.

b. System Administrator

    i. Installs, manages, and maintains IT systems;

    ii. Documents system technical requirements;

    iii. Develops system-level plans using forms and resources provided by the IT Security Department; and

    iv. Validates system-level procedures.

c. IT Security Department

    i. Oversees the Disaster Recovery process;

    ii. Develops and publishes the District-level DR plan and supporting documentation, including a Critical Asset List (CAL) and Communications Management Plan;

    iii. Develop standardized templates, forms, and supporting documents for system-level plans;

    iv. Reviews system-level plans as necessary; and

    v. Coordinates with System Owners and Administrators to ensure that they understand and acknowledge established Disaster Recovery plans.

d. Chief Information Officer

    i. Oversees the District's IT Disaster Recovery Response efforts; and

    ii. Allocates shared resources based on business priorities.

e. Office of Information Technology

    i. Maintains the District Configuration Management Database (CMDB); and

    ii. Creates a Disaster Recovery plan for restoring common IT infrastructure.

2. Disaster Recovery Planning

    a. The Office of Information Technology must create and maintain a District IT Disaster Recovery Plan that identifies and protects against risks to critical systems and sensitive information in the event of a disaster.

    b. The District IT Disaster Recovery Plan must provide for contingencies to restore information and systems if a disaster occurs based on the business priorities across all District departments. Priorities are determined based on compelling operational, compliance or security needs of the organization.

    c. The Office of Information Technology must maintain a centralized inventory of all District Information Resources, commonly known as a Configuration Management Database (CMDB). Using the CMDB, the District may begin to map business functions to their supporting IT systems to prioritize Disaster Recovery resources and prioritize recovery efforts.

    d. All systems dependencies including hardware, software, and data must be inventoried to ensure that all requirements can be met to support business critical systems.

3. Business Impact Assessments (BIA)

    a. A BIA must be performed for each business function by the responsible department including system owners and supporting personnel.

    b. BIA identify the duration of an outage to a business function before negative impacts (or costs) to the organization are realized. Costs may be:

        i. Financial

            1) Lost time (business unit or supporting employees);

            2) Technical recovery costs;

            3) Legal/Regulatory fines;

        ii. Reputational

            1) Customer/Community dissatisfaction;

            2) Negative public reputation;

            3) Loss of staff morale;

iii. Operational/Customer

1) Data loss/corruption;

2) Supply chain interruption;

3) Delay to plans or work;

4) Contractual penalties; or

iv. Legal/Regulatory

1) Failure to comply with regulations.

c. After BIA are performed, the IT Security Department must review consolidated BIAs, associated system requirements and inventories, and develop a Business Impact Analysis report.

d. Using the BIA report, the IT Security Department must develop a proposed District Critical Asset List (CAL). The CAL must be distributed to District leadership and documented in the District Disaster Recovery Plan.

4. Disaster Declaration

a. A disaster declaration activates the Disaster Recovery Plan. Ordinary circumstances and processes are bypassed to ensure that systems can be restored to an operational state. Typical workflows, like Configuration Management or customer notification, may be bypassed from typical approval requirements.

b. Any of the following can declare a disaster:

i. Superintendent, or designee;

ii. Deputy Superintendent, or designee;

iii. Chief Information Officer, or designee;

c. The person who declared the disaster can declare when a disaster is over and normal operations can resume.

5. Employee Training and Acknowledgement

a. Employees must be informed of and acknowledge their responsibilities included in Disaster Recovery Plans.

b. Employees must receive role-specific training that prepares them for their responsibilities during a Disaster scenario.

6. Plan Testing and Validation

    a. Disaster Recovery Plan testing and validation must be performed regularly to ensure that procedures are current and continuously improved, and key personnel are trained on their responsibilities.

    b. Testing

        i. Testing involves a reviewing the plan to ensure that the procedures are practical, realistic, and relevant to system recovery in a disaster scenario; and

        ii. Testing can be performed in many ways. Key personnel may perform one or more of the following exercises:

            1) Read-through;

            2) Walk-though;

            3) Simulation;

            4) Parallel; or

            5) Full interruption.

    c. Validation

        i. The validation process ensures that the plan is still relevant despite system changes that have occurred since the last review; and

        ii. If plans need to be changed, they may be updated with changes being tracked and documented in the Disaster Recovery Plan Change Log. All personnel assigned to the plan must be notified to ensure that they review and accept the changes.

    d. All Disaster Recovery Plan must be validated semi-annually; testing must be performed annually.

    e. All plan testing and validation activities must be scheduled with results documented in writing.

LEGAL REQUIREMENTS AND ASSOCIATED DOCUMENTS

1. This Administrative Regulation reflects the goals of the District's Strategic Plan and aligns/complies with the governing documents of the District, to include:

    a. Board Policy 7205, Information Technology – Data Access; and

    b. Administrative Regulation 7211, Responsible Use and Internet Safety.

REVISION HISTORY

Date	Revision	Modification
06/15/2022	1.0	Adopted