Runge Independent School District

Technology Disaster Recovery Plan (TDRP)

Board Approved: May 2013

Information Technology Statement of Intent

This document delineates our procedures for technology disaster recovery, as well as our process-level plans for recovering critical technology platforms and telecommunications infrastructure. This document summarizes our recommended procedures. In the event of an actual emergency situation, modifications to this document may be made to ensure physical safety of our students, staff, systems, and data.

Our mission is to ensure information system uptime, data integrity, data availability, and business continuity.

- The District shall develop a comprehensive Technology Disaster Recovery Plan (TDRP).
- The TDRP should cover all essential and critical infrastructures elements, systems and networks, in accordance with key business activities.
- The TDRP is to be kept up to date to take into account changing circumstances.

Objectives

The principal objective of the TDRP is to develop, test and document a well-structured and easily understood plan which will help the District recover as quickly and effectively as possible from an unforeseen disaster or emergency which interrupts information systems and/or business operations.

Additional objectives include the following:

- The need to ensure that employees fully understand their duties in implementing such a plan
- The need to ensure that operational policies are adhered to within all planned activities
- The need to ensure that proposed contingency arrangements are cost-effective

Key Personnel Contact Information

Name	Phone Number	Email Address
Linda Bettin Superintendent	830-239-4315 X 204	lbettin@rungeisd.org
Pete Ybarra Director of Maintenance & Transportation	830-239-4315 X 503	ybarrap@rungeisd.org
Aiden Everett Technology Director	830-239-4315 X 108	everetta@rungeisd.org
Randy Ramirez Business Manager	830-239-4315 X 206	ramirezr@rungeisd.org
Brenda De La Rosa Principal	830 -239-4315 X 106	bdelarosa@rungeisd.org

External Contacts

Region 3 ESC- Technical Support & ISP	Phone Number	361.573.0731
AT&T Ticket Express - ISP Backbone Carrier	Website	https://expressticketing.acss.att.com
SOCS – Web Hosting	Phone Number	800.850.8397 x 3
	Email Address	SOCSSupport@fes.org
Keep it Safe – Offsite Daily Server Backup	Phone Number	888.676.0300
	Email Address	support@keepitsafe.com
AT&T Landline Telephone Business Repair	Phone Number	800.246.8464
Flexile Technologies Systems - Consultant	Phone Number	210.616.2886

1 Plan Overview

1.1 Plan Updating

The TDRP updating process needs to be properly structured and controlled. Whenever changes are made to the plan they are to be fully tested and appropriate amendments should be made to the TDRP. This will involve the use of formalized change control procedures under the direction of the Technology Coordinator.

1.2 Plan Documentation Storage

Copies of this plan will be stored in secure locations to be defined by Runge ISD and shared as a Google Document within the rungeisd.org domain.

1.3 Backup Strategy

Business processes and the agreed backup strategy for each are listed below. If the chosen strategy is for a fully copied, off- site backup, this data will be stored in an off-site facility away.

PROCESS/VENDOR	BACKUP
Domain Controller 1	Fully copied, Off-Site Backup
Domain Controller 2	Fully copied, Off-Site Backup
Telephone Server Voice and Data	Fully copied, Off-Site Backup
TimeQPlus Time Clock User Data	Fully copied, Off-Site Backup

1.4 Risk Management

There are potential disruptive threats which can occur at any time and affect the normal business process. We have considered a wide range of potential threats and the results of our deliberations are included in this section. Each potential environmental disaster or emergency situation has been examined. The focus here is on the level of business disruption which could arise from each type of disaster.

Potential disasters have been assessed as follows:

Potential	Probability Rating	Impact Rating	Description of Potential Consequences & Remedial Actions
Flood	4	3	All critical equipment is located on 1st floor.
Fire	4	2	
Tornado	5	2	
Electrical storms	5	3	Use of surge protectors/UPS devices on all servers.
Hurricane	4	3	
Act of sabotage	5	3	
Electrical power failure	3	3	UPS devices are used to help with quick power outages.
Loss of communications	3	3	Contact AT&T if issue is external of RISD.

Probability: 1 – Very High, 5 – Very Low; Impact: 1 – Total Destruction, 5 – Minor Annoyance

2.0 Emergency Response

2.1 Alert, escalation and plan invocation

2.1.1 Plan Triggering Events

Key trigger issues that would lead to activation of the TDRP are:

- Total loss of all communications for more the 8 hours
- Total loss of power for more than 8 hours
- Flooding of the premises
- Loss of the building
- Fire effecting network equipment or communications

2.1.2 Assembly Points

Where the premises need to be evacuated, the TDRP follows current evacuation plan in place by RISD.

2.1.3 Activation of Emergency Response Team

- When an incident occurs the Emergency Response Team (ERT) should be activated. The ERT will then decide the extent to which the TDRP should be invoked. Responsibilities of the ERT are to:
- Respond immediately to a potential disaster
- Assess the extent of the disaster and its impact on the business, data center, etc.

- Decide which elements of the TDRP should be activated
- Establish and manage disaster recovery team to maintain vital services and return to normal operation
- Ensure employees are notified and allocate responsibilities and activities as required

2.2 Disaster Recovery Team

The team's responsibilities include:

- Try to establish facilities for an emergency level of service within 8.0 business hours
- Try to restore key services within 8.0 business hours of the incident
- Try to recover to business as usual within 8.0 to 48.0 hours after the incident
- Report to the Administration

2.3 Emergency Alert, Escalation and Disaster Recovery Plan Activation

This policy and procedure has been established to ensure that in the event of a disaster or crisis, personnel will have a clear understanding of who should be contacted. Procedures have been addressed to ensure that communications can be quickly established while activating disaster recovery.

The TDRP will rely on key members of management and staff who will provide the technical and management skills necessary to achieve a smooth technology and business recovery. Suppliers of critical goods and services will continue to support recovery of business operations as the District returns to normal operating mode.

2.3.1 Emergency Alert

The person discovering the incident calls a member of the Emergency Response Team in the order listed:

- Emergency Response Team
- Technology Director
- Superintendent
- Principal/Assistant Principals
- Maintenance/Transportation Director
- Business Manager

The Emergency Response Team (ERT) is responsible for activating the Disaster Recovery Plan for disasters identified in this plan, as well as in the event of any other occurrence that affects the District's capability to perform normally.

One of the tasks during the early stages of the emergency is to notify the Disaster Recovery Team (DRT) that an emergency has occurred. The notification will request DRT members to

assemble at the site of the problem and will involve sufficient information to have this request effectively communicated.

2.4 Coordination with First Responders

- Coordination with local law enforcement and EMS Centers as needed
- Sustaining awareness of restricted movement and curfew conditions (ensuring staff are traveling when allowable).
- Reporting of service restoration progress to Federal, State and Local authorities as needed

3 Media

3.1 Media Contact

The Superintendent of Schools or Designee will be the sole communicator for all media, working according to guidelines that have been previously approved and issued for dealing with post-disaster communications.

3.2 Media Strategies

Have answers to the following basic questions:

- What happened?
- How did it happen?
- What are you going to do about it?

3.3 Media Team

The Superintendent of Schools or Designee will be the sole communicator for all media.

4 Financial

4.1 Financial Assessment

The emergency response team shall prepare an initial assessment of the impact of the incident on the financial affairs of the District and report their findings to the Business Manager. If applicable, the assessment should include:

- Loss of hardware costs
- Labor cost
- Consultant costs
- Costs of new Hardware

5.0 Data Loss Prevention

To prevent data loss from a disaster, the IT Department will follow all disaster policies and guidelines set forth by the Runge ISD. In addition, the IT Department along with Keep it Safe-offsite data backup, will create daily backups to protect and restore server data for on-site systems by performing backups and restoring backups.

5.1

In the event of immediate threat, the IT Department will take the following actions:

- Backups will be performed daily and stored offsite by Keep it Safe.
- Most servers except mission critical servers (Active Directory) will be shut down.
- Information will be provided on the Runge ISD web site and social media outlets.
- Network closets and battery backups (UPS) should be turned off if unnecessary

5.2

Every classroom, computer lab, and district office department should take the following steps to protect data and equipment:

- Computers should be turned off and unplugged, if connected to battery backups there should be turned off and unplugged as well.
- Computers should be moved away from windows, off the floor, and covered with plastic if possible.

6.0 Purchasing

The IT department is responsible for the seamless integration of any hardware or software into the existing network system. When considering the purchase of any technology related item, prior approval from the IT Department is required.

7.0 Revisions

The Runge ISD School Board reserves the right to change these policies and procedures at any time to ensure the operability and safety of the network and its users.