

## Risk Management Plan

Our risk management plan has been developed in accordance with the guidelines developed by the State of Texas Department of Information Resources.

We have also applied the broad experience of other school networks in Texas to help us understand and evaluate the risks that we face in our own community.

Our contingency plan describes how we will respond to unplanned outages of service. Our plan provides a proactive guide for our community network to employ to ensure that we will restore normal service quickly, efficiently, and cost effectively.

### Step 1. Obtain Commitment from Executive Management.

We met with our Schleicher County ISD administrators and presented them with the reasons for examining disaster recovery. We explained that the resources needed for proper contingency planning included their time and support, staff awareness and involvement, and multi-agency collaboration on community network risk and recovery issues.

The SCHLEICHER COUNTY ISD was very supportive and willing to provide the necessary resources for developing and implementing the plan and for continuous monitoring and updating of the contingency plan.

### Step 2. Establish a Services Resumption Planning Committee.

The SCISD Technology Director will designate our members of the planning committee. These members will represent all of the primary collaborators on the community network project. This team developed the components of the contingency plan. The team will meet yearly, or more often if necessary, to review, update and continuously improve the contingency plan. The team will report to the SCHLEICHER COUNTY ISD Superintendent.

### Step 3. Perform a Service Resumption Capability Assessment.

One of the tools used by the team to assess risk is the "Service Resumption Capability Checklist" (see Appendices). In addition to evaluating current locations, this checklist is also useful for selecting new public access and server locations. All equipment will be inventoried at the time of delivery and inventories verified quarterly. When evaluating capabilities using the checklist, any deficiencies will be assigned to personnel from the collaborative for action. The results of the checklist review will be included in the quarterly reports to the SCHLEICHER COUNTY ISD School Board.

### Step 4. Perform a Risk Analysis.

The top risks for our community network are identified in the table below. We employed the risk assessment and management approach recommended by the State of Texas (DIR). We inserted the risks we identified into the following table (from the Software Quality Institute at the University of Texas) for analysis of specific risks.

## Risk Analysis for Project, Planning, Implementation and Operations

Risk Item	Prob <sup>1</sup>	Loss <sup>2</sup>	Risk Exposure <sup>3</sup>	Resolution Approach	Who
Loss of match funding	20	10	200	Continually monitor and seek donations to fund	
Natural disaster: flood, fire, etc.	5	10	50	Work with local public safety for maximum prevention	
Internet security breach	30	3	90	Monitor firewall protections	
Technical failure: network downtime, server inaccessible	40	10	400	Backup all key files daily; 24 hour personnel and vendor call list	
Technology becomes incompatible (e.g. wireless components no longer work with equipment)	40	10	400	Ensure compatibility upgrades by contract where possible; monitor industry trends	
Theft, vandalism	20	5	100	Develop community sense of ownership to minimize theft; keep sites secure	
Loss of project partner or project team difficulties	20	2	40	Continuous communication with partners; share responsibilities of all partners so that the loss of one is of no effect	
Project behind schedule	80	3	240	Monitor progress; see problems early	
Loss of key staff	20	8	160	Cross train staff and volunteers	

Trainers and volunteers are less available than expected	30	5	150	Implement ongoing train the trainer programs to maintain adequate pool of volunteers	
Public access facilities use is low	40	6	240	Develop community trust; Communicate accessibility and hours; provide services according to community feedback	
Some local businesses see community network as interloper into private sector space	20	5	100	Involve local businesses in community network; complement not duplicate private sector services	
Loss of support of local business sector (e.g. Chamber of Commerce)	10	5	50	Involve local chamber, key businesses in community network decision-making.	

1

Probability of unsatisfactory outcome on a scale of 0-100 with 100 being the most likely to occur.

2

Projected loss should unsatisfactory outcome occur on a scale of 0-10 with 10 being the most loss

3

Risk Exposure is the probability of unsatisfactory outcome times the loss if the outcome is unsatisfactory

**Step 5. Establish System Priorities.**

In addition to examining risks associated with the community networking project planning and implementation, DIR and TIF recommend analysis and management of risks that are specific to applications and software related services. The following table lists and assesses the primary risks we have identified that are related to software and web services. These risks are in addition to the risks identified previously in this risk management plan.

## Risk Analysis for Specific Automated Software Applications, Web Services

Risk Item	Prob <sup>1</sup>	Loss <sup>2</sup>	Risk Exposure <sup>3</sup>	Resolution Approach	Who
Web server is unavailable; network is up but web site is down	30	3	90	Provide emergency personnel call list; Provide redundant hosting for local web site	
File transfer (FTP or SCP) services are down and local site cannot be remotely updated	40	2	80	Ensure physical access to server so that updates can happen at the machine itself using a disk or CD	
Local site web content destroyed (hardware failure or hack, crack)	50	10	500	Backup all files regularly and store backups for at least 1 week; maintain offsite backup	
Server facility becomes inaccessible	5	10	50	Arrange for backup hosting or delay access until site is available	
Telecommunications central facility becomes inaccessible	5	10	50	Re-route through the school district's T; secure a phone number with a recording that can be called by customers for network status	

1

Probability of unsatisfactory outcome on a scale of 0-100 with 100 being the most likely to occur.

2

Projected loss should unsatisfactory outcome occur on a scale of 0-10 with 10 being the most loss  
Risk Exposure is the probability of unsatisfactory outcome times the loss if the outcome is

unsatisfactory

Step 6. Analyze and Define Requirements for Recovery

We have defined many of the strategies and tactics for recovery and prevention in the table above. Specific requirements for recovery include:

- Develop policies and procedure for public information in the event of a lengthy outage
- Regular, systematic backup of all web site files and scripts
  
- Develop and communicate a list of key emergency personnel
- Maintain backup copies for at least the past 5 days
- Security monitoring 24 hours a day 7 days a week of all servers
- Comprehensive firewall protection for all servers and networks
- Train the trainer programs to ensure staff and volunteer availability
- Trained backup personnel for all system administrators

-

Step 7. Design the Program for Recovery Operations. In our community, the SCHLEICHER COUNTY ISD will assign a Recovery Coordination Team. The team is responsible for coordinating all aspects of a recovery operation. Once our services are all in place, we will further define the specific responsibilities and procedures that the team will follow. Specific procedures will be developed which will include at least the following elements:

- A list and description of each procedure
- Purpose of each procedure
- Scope of the procedure, what it involves
- Specific authority for the procedure.
  
- Specific responsibilities for each procedure.
- Steps for each procedure will be detailed.

Step 8. Conduct Service Resumption Training.

The Recovery Coordination Team will hold quarterly training for service resumption. This training will be conducted after the quarterly review and update of this risk management plan. Providing adequate training to key personnel is vital to the success of resource recovery. Successful execution of a service resumption situation largely depends on how well the responsible personnel are trained and ready to execute the resumption processes. All key personnel will be cross-trained.

Step 9. Test the Service Resumption Plan.

As we have indicated previously, the risk management plan and recovery operations procedures will be thoroughly reviewed and tested quarterly. We will evaluate the response to the emergency and update plan, procedures and training as needed to mitigate any faults.

Step 10. Maintain and Update the Service Resumption Plan.

As we have indicated previously, the Recovery Coordination Team will conduct quarterly reviews and updates of the risk management plan and recovery operations procedures and policies. Should we experience turnover of key staff, the reviews will occur more frequently to ensure that no gaps in our ability to manage risks occur.

## Disaster Recovery and Response

### **Fault Tolerance**

SCHLEICHER COUNTY ISD mission critical equipment will be RAID 5 hot swappable servers with one possessing a tape Dell PowerVault 8 tape storage plus USB 320 gig IDE drives. UPS 1400(min) battery backups will provide fault tolerance for electrical circuits. Backup servers will backup critical data to off-site servers at the SCISD as well as store monthly tape backups off site at the SCISD fire-proof vault.

### **Disaster Detection and Determination**

The detection of an event which could result in a disaster affecting information processing systems at the SCHLEICHER COUNTY ISD is the responsibility of SCISD systems administrator and Major Disaster Team. The Disaster Team will consist of SCISD technical personnel as well as some local vendors.

### **Disaster Notification**

SCISD systems administrator will follow existing procedures and notify the individuals who are acting as technical consultants or SCISD technical personnel.

### **Disaster Recovery Strategy**

The disaster recovery strategy explained below pertains specifically to a disaster disabling the main data center (i.e.; tornado, fire, act of god). This functional area (MDF) provides mission critical systems that are especially at risk and contain the critical applications of those designated as Category I (see below) systems. This section

addresses three phases of disaster recovery:

- o Emergency
- o Backup
- o Recovery

Strategies for accomplishing each of these phases are described below. It should be noted that the subsection describing the emergency phase applies equally to a disaster affecting the SCHLEICHER COUNTY ISD or the functional area that provides support for the maintenance of the critical system.

### **Emergency Phase**

The emergency phase begins with the initial response to a disaster. During this phase, the existing emergency plans and procedures for SCHLEICHER COUNTY ISD are enlisted through existing mechanisms. The Major Disaster Team is alerted by pager and begins to monitor the situation. If the emergency situation appears to affect (MDF) (or other critical facility or service), either through damage to data processing or to support facilities, or if access to the facility is prohibited, then the system administrators will closely monitor the event, notifying contract technical associates, and law enforcement as required to assist in damage assessment. Once access to the facility is permitted, an assessment of the damage is made to determine the estimated length of the outage. If access to the facility is precluded, then the estimate includes the time until the effect of the disaster on the facility can be evaluated. If the estimated outage is less than 12 hours, recovery will be initiated under normal Information Systems operational recovery procedures. If the outage is estimated to be longer than 12 hours, then the System Administrators move into the back-up phase. The Disaster Team will remain active until recovery is complete to ensure that the network will be ready in the event the situation changes.

### **Back-up Phase**

The back-up phase begins with the initiation of the appropriate. Processing will resume

either at the main data center or at the designated hot site, depending on the results of the assessment of damage to equipment and the physical structure of the building. In the backup phase, the initial hot site (SCISD SECONDARY SYSTEM) must support critical applications. During this period, processing of these systems resumes, possibly in a degraded mode, up to the capacity of the hot site. Within this period, the main data center will be returned to full operational status if possible.

## **Recovery Phase**

The time required for recovery of the functional area and the eventual restoration of normal processing depends on the damage caused by the disaster. The time frame for recovery can vary from several days to several months. In either case, the recovery process begins immediately after the disaster and takes place in parallel with backup operations at the designated hot site. The primary goal is to restore normal operations as soon as possible.

## **Recovery Procedures**

### Action Procedures

Building Services will notify team members and vendors to report to the site for initial damage assessment and clean-up.

Physical Plant Administrator will notify insurance representative.

Operations Center will issue work orders and call appropriate personnel.

Disaster Team Leader will request permission to enter site from Fire Department (if required).

Take a service representative from each of the appropriate vendors, the insurance claims representative, and appropriate Information Systems personnel into the site.

Disaster Team Members will review and assess the damage to the facility. List all equipment and the extent of damage and list damage to all support systems (power, A/C, fire suppression, communications, etc.).

Team Leader will notify the Disaster Team as to the severity of the damage and what can potentially be salvaged.

### Salvage Operations

Team Leader will initiate the Emergency Notification List and have all members report to the Staging Area. Salvage Team Have the Building Services Supervisor determines which equipment and furniture can be salvaged. Photograph all damaged areas as soon as possible for potential insurance claims.

Have the Physical Plant Supervisor and staff starts salvaging any furniture and equipment. Based upon advice from the Insurance Team and customer engineering, the supervisor will contact computer hardware refurbishers regarding reconditioning of damaged equipment.

## Action Procedures

When an emergency occurs:

The Public Information Officer (as appointed by the SCHLEICHER COUNTY ISD board or SCISD) will assess the public relations scope of the emergency, in consultation with senior management if necessary, and determine the appropriate public relations course of action.

In instances where media are notified immediately, due to fire department or police involvement, the Public Information Officer will proceed to the scene at once to gather initial facts. Emphasis must be placed upon getting pertinent information to the news media as quickly as possible.

Public Information Officer maintains a log of all information which has been released to the media.

Public Information Officer, when appropriate, prepares news releases on a periodic basis for distribution to the local media list.

Public Information Officer will, if employee injuries or fatalities are involved, notify personnel to send appropriate management personnel to the homes of the involved families.

Personnel must notify Public Information Officer as soon as families have been

informed. This will permit the release of names and addresses of victims so that families of those not involved can be relieved of anxiety.

Public Information Officer must contact the public relations director(s) at the hospitals where the injured have been taken to coordinate the release of information.

Public Information Officer must, in cases where long-term media coverage is anticipated, establish a Press Room in a location to be selected. Telephone requirements for the press must be provided.

Public Information Officer schedules periodic press conferences, taking into consideration management personnel who will be participating.

Public Information Officer must clear media request to photograph physical damage and accompany all photographers.

• Public Information Officer coordinates follow-up news releases after the immediate emergency has passed to present the network in as positive a light as possible. Possible topics could include:

- o What has been done to prevent recurrence of this type of emergency?
- o What are plans for reconstruction?
- o What has been done to express gratitude to the community?
- o What has been done to help employees, students and faculty?

## **DISASTER RECOVERY CAPABILITY ASSESSMENT CHECKLIST**

### **ACCESS CONTROL**

\_\_\_ Location:

not a target for vandals

close to emergency response units (e.g., Fire Dept.)

not close to rail lines

not close to manufacturing or chemical plants

not close to research facilities with toxic waste

not close to landfills

\_\_\_ Guards, receptionists or someone monitoring entrances \_\_\_ Sign-in log at entrances

\_\_\_ Policy to challenge unfamiliar visitors \_\_\_ Entrance security devices for after hours access requiring keys, pass-codes or magnetic badges \_\_\_ Security awareness training

program for employees and volunteers \_\_\_ Published security policy/procedures \_\_\_  
Require positive identification of vendor personnel \_\_\_ Collect keys and/or badges  
and/or change codes when employees or volunteers terminate

### **FLOOD CONTROL**

**Date Checklist Reviewed:** \_\_\_\_\_ **By Whom:**

- \_\_\_ Equipment located above water grade
- \_\_\_ Steam or water pipes located below computer room
- \_\_\_ Adequate water drainage in computer rooms and in adjacent areas
- \_\_\_ Inform employees of location of water pipe shut-off valves
- \_\_\_ Sealed windows

### **HOUSEKEEPING**

- \_\_\_ Flammable materials properly stored
- \_\_\_ Area cleaned regularly
- \_\_\_ Paper, supplies and trash stored outside computer area
- \_\_\_ No asbestos on utility steam pipes
- \_\_\_ A *no smoking* policy in the equipment room

### **FIRE CONTROL**

- \_\_\_ Fire resistant/noncombustible materials used for the building, partitions, walls, doors
- \_\_\_ Smoke or heat detectors installed \_\_\_ Smoke detector system tested periodically
- \_\_\_ Fire extinguishers easily accessible, with type and use identified, inspected regularly
- \_\_\_ Staff and volunteers trained in use of fire extinguishers \_\_\_ Date of last training
- \_\_\_ Established current emergency fire procedures and evacuation plan \_\_\_ Post fire department's phone number on/near each phone \_\_\_ Close liaison established with the local fire department \_\_\_ Training for all employees in fire prevention \_\_\_ Smoking restricted in the computer area \_\_\_ Fire alarms tested every 12 months \_\_\_ Emergency exit diagrams posted near all exits \_\_\_ Regular fire prevention inspections \_\_\_ Fire exits clearly identified and kept open \_\_\_ Audible and visible alarms \_\_\_ No PVC cabling in hidden areas (walls, above ceiling)

### **ELECTRICAL POWER**

\_\_\_ Reliable electrical power \_\_\_ Emergency lights installed and working

### **CLIMATE CONTROL**

\_\_\_ Controlled humidity \_\_\_ Preventive maintenance schedule observed

### **PERSONNEL CONSIDERATIONS**

\_\_\_ Controls established for departing employees and volunteers \_\_\_  
Personnel policies and procedures available

### **HARDWARE CONSIDERATIONS**

\_\_\_ All periods of reported downtime logged \_\_\_ Preventive maintenance schedule observed \_\_\_ Offsite storage of all hardware inventory and documentation

### **SOFTWARE CONSIDERATIONS**

\_\_\_ All original software (disks, CDs) and documentation secured \_\_\_ Offsite storage of all software inventory and license and support information \_\_\_ Backup files stored off-site regularly \_\_\_ Servers - Restricted access to operating and production software \_\_\_ Servers

- Access to systems software limited and monitored \_\_\_ Servers - Security software and access codes validated \_\_\_ Servers - Passwords used to identify system administration users \_\_\_ Servers - Passwords changed every 6 months or more frequently as needed \_\_\_ Servers - Restart/recovery procedures for web services and application programs \_\_\_ Servers - Configuration change documentation and control

### **COMMUNICATIONS CONSIDERATIONS**

\_\_\_ All communications lines documented and records of cabling plan offsite \_\_\_ Offsite storage of all equipment inventory and documentation \_\_\_ System use log verified periodically \_\_\_ Network control function password protected \_\_\_ Access to the network control center restricted \_\_\_ Communications and network failure troubleshoot/correction procedures \_\_\_ Vendor list for trouble calls available and regularly updated \_\_\_ All network circuits and outlets named and marked

### **CONTINGENCY PLANNING**

\_\_\_ Formal written contingency plan available \_\_\_ Contingency plan training regularly conducted \_\_\_ Back-up server available \_\_\_ Contingency plan tested on yearly basis

### **PUBLIC ACCESS COMPUTER INSTALLATIONS**

\_\_\_ Equipment/network configurations documented/standardized \_\_\_ Equipment and/or network configurations stored offsite \_\_\_ Back-up public access computer available \_\_\_ Viral prevention installed \_\_\_ System configuration (e.g. control panels) write protected \_\_\_ Standard back-up procedures \_\_\_ Offsite storage of data, software, and documentation

## **Equipment Replacement and/Or Upgrade**

PC and Servers have three year onsite warranties  
Switches will possess 24 hour Smart-Net Maintenance  
Upgrade of software will be determined on cost of volume licensing versus performance changes or upgrades – (we will not replace software just because it is new-existing software must be obsolete by business industry standards).

## **Disposal Strategy**

Future disposition of any SCISD equipment or other assets determine to be obsolete or unneeded, will be made in full compliance with policies and regulations of the fiscal agent and the state.