Kimberly School District # 414

Technology Disaster Recovery Plan (TDRP)

Table of Contents

Information Technology Statement of Intent

This document conveys 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).
- A risk assessment shall be undertaken to determine the requirements for the TDRP.
- The TDRP should cover all essential and critical infrastructures elements, systems and networks, in accordance with key business activities.
- The TDRP should be tested annually to ensure that it can be implemented in emergency situations and that the management and staff understand how it is to be executed.
- All staff must be made aware of the TDRP and their own respective roles.
- 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 KSD 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 all 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	Position	Phone Number	Email Address
Luke Schroeder	Superintendent	208.423.4170 x3308/3310 208.420.1344	lschroeder@kimberly.edu
Keelie Campbell	Director of Programs	208.423.4170 x3325 208.539.5530	kcampbell@kimberly.edu
Ted Wasko	Director of Maintenance	208.423.4170 x3300 208.961.0515	twasko@kimberly.edu
Patty Dame	Technology Supervisor	208.423.4170 x3312 208.731.4371	pdame@kimberly.edu
Harrison Huttanus	Network Manager	208.423.4170 x3323 208.404.1040	hhuttanus@kimberly.edu
Kathi Johnson	Help Desk Specialist	208.423.4170x3322 208.421.0599	kjohnson@kimberly.edu
Darla Wadsworth	Director of Transportation	208.423.4170 x3328 208.731.8302	dwadwsorth@kimberly.edu
Nate Bondelid	Tek-Hut Contact (Filter/Internet)	208.377.5159 208.421.6261	nate@tek-hut.com
Daniel Hart	Tek-Hut Contact (Filter/Internet/O365)	208.327.5755 208.320.8497	daniel@tek-hut.com
Mike Nelson	Tek-Hut Local Contact	208.735.5159	m@tek-hut.com

External Contacts

Redacted for online security		

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 training materials. This will involve the use of formalized change control procedures under the direction of the Technology Supervisor or Network Manager.

1.2 Plan Documentation Storage

Copies of this plan will be stored in secure locations to be defined by Kimberly School District and shared as a Word Document within the Leadership Team O365 Group as well as within the Tech Department. Key Personnel will be issued a hard copy of this plan to be filed at home.

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. If the chosen strategy is for a fully copied, on-site backup, this data will be stored in a separate location than the current production copy.

Vendor	BackUp
PowerSchool Student Information System	*Fully copied, off-site Backup*
Tyler Technologies Infinite Vision (CSA)	*Fully copied, off-site Backup*
Aerohives	
Hosted Services: Destiny	
Canvas	
HVAC	
Sprinklers	

1.4 Risk Management

There are potential disruptive threats which can occur at any time and affect the normal business process. 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	Probability Rating	Impact Rating	Description of Potential Consequences & Remedial Actions
Cyberthreat	1	2	Shut off network
Electrical Power Failure	2	4	UPS devices are used to help with quick outages
Loss of Phone Communications	3	3	Utilize Radios/Cell Phones
Sabotage	4	3	Repair/Replacement of equipment/services
Electrical Storms	3	3	Use of surge protectors on all servers to protect from damage
Flood	5	3	All critical equip. is located on 1st floor
Fire	5	3	Total loss/no services. Move to new site.

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 than 8 hours
. Total loss of power for more than 8 hours
. Flooding of the premises
. Loss of the building
. Fire affecting network equipment or communications

2.2 Disaster Recovery Team

The team's responsibilities include:

. Establish facilities for an emergency level of service within 8 business hours;
. Restore key services within 8 business hours of the incident;
. Recover to business as usual within 8 to 48 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:

- District Administration (Superintendent)
- Technology Supervisor/Network Manager
- Principal/Assistant Principal (In building affected)
- Maintenance Director
- Transportation Director

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. Members of the team should assemble at the site of problem if able

or either the District office or KHS office and be ready to put plans in motion.

2.4 Coordination with First Responders (If a physical/structural emergency)

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

3.0 Media

Assigned staff will coordinate with the media, working accordingly to guidelines that have been previously approved and issued for dealing with post-disaster communications.

3.1 Media Strategies

Have answers to the following basic questions ready:

- What happened?
- How did it happen?
- What is the District going to do about it?

4.0 Financial and Legal Issues

4.1 Financial Assessment

The ERT shall prepare an initial assessment of the impact of the incident on the financial affairs of the District and report their findings to the Superintendent. The assessment should include:

- Loss of hardware costs
- Labor cost
- Consultant costs

5.0 Security Incidents

5.1 Definition

A security incident is any violation of set Policies and Procedures that may or may not result in the following:

- loss of information confidentiality (data theft)
- compromise of information integrity (damage to data or unauthorized modification)
- theft of physical technology asset including computers, storage devices,

printers, etc.

- denial of service
- misuse of services, information, or assets
- infection of systems by unauthorized or hostile software
- an attempt at unauthorized access
- unauthorized changes to organizational hardware, software, or configuration
- reports of unusual system behavior etc.

5.2 Response

If a KSD Technician becomes aware of a security incident, they must provide notification of the incident to the Technology Supervisor or Superintendent. Upon confirmation, the Technology Supervisor will notify the user's supervisor (if a KSD employee) or School Administrator (if a KSD student).

Other steps that must be taken:

- Temporarily suspend or restrict the user's computing privileges during the investigation. Reactivation is the discretion of the Employee's supervisor or Student's school administrator.
- Isolate the infected computer immediately: Infected systems should be removed from the network as soon as possible to prevent ransomware from attacking network or shared devices.
- Immediately secure backup data or systems by taking them offline: Ensure that all backups are free of malware.
- Contact KSD's Insurance company immediately. Contact Law Enforcement if necessary.
- If available, collect and secure partial portions of the ransomed data that might exist for forensic investigations to check for exfiltration of data.
- If possible, change all online account passwords and network passwords after removing system from the network. Change all system passwords once the malware is removed from the system

These steps may be taken only after authorization by the Superintendent or Technology Supervisor unless the situation represents an emergency or immediate threat to network security/integrity. In such case, the Network Manager (or other technician in his absence) must take corrective action and notify the Technology Supervisor as soon as possible. Actions should be taken in such a way that any impacts to non-offending users are minimized.

5.3 Monitoring

In an effort to maintain network security, integrity, and to reduce the risk of Security Incidents the KSD Technology Department along with the Tek-Hut may monitor network activity by means including but not limited to:

- Firewall logs
- Web filtering logs
- Network Traffic Monitoring
- Active Directory Monitoring and Auditing of Accounts
- Usage Logs
- Event logs and histories as needed

5.3.1 Files and Correspondence

It may be necessary for KSD Network Manager (or other employee designated by Tech supervisor or other KSD Admin) or Tek-Hut to view files, data or communications that have been stored by users on devices or network file servers. The viewing of such material is permitted only when it is necessary to troubleshoot problems at the request of the user (or district administrators), protect the security and integrity of KSD's network, protect the rights or property of KSD or third parties, or to ensure compliance with KSD policy or applicable law. Examples include:

- The identification/restoration of lost, damaged or deleted files
- The identification of a process that is interfering with normal network functions
- In more serious circumstances, an investigation of a Security Incident

In all such cases, the KSD Network Manager (or other KSD Employee, as stated above) shall take into consideration the confidential nature of files and/or communications that may potentially be reviewed and shall implement the appropriate safeguards to ensure that all local, state and federal privacy laws are complied with. The Technology Supervisor and/or Superintendent must be advised of and approve any non-routine monitoring that occurs. Non-routine monitoring includes directed investigations of potential policy and/or security violations. Discovery of such violations in the course of routine monitoring must be reported.

6.0 Data Loss Prevention

6.1 Physical Disaster Preventions

To prevent data loss from a physical disaster, the KSD Technology Department will follow all disaster policies and guidelines set forth by KSD. In addition, the KSD Technology Department will take routine measures to protect and restore data on-site systems by performing backups and storing backups. Contracts for information systems off-site include data loss protection plans and disaster recovery plans.

In the event of an immediate threat, the KSD Technology Department will take the following actions:

- Backups will be performed and stored in multiple locations
- Most servers except mission critical servers (Active Directory) will be shut down.
- Information will be provided on the KSD website
- Network closets and battery backups (UPS) should be turned off if unnecessary
- In the event the Technology Department Building (or other buildings containing servers) is damaged or destroyed, operations will be re-established at one of the others school buildings or off-site with the help of KSD's outsourced internet provider (currently Tek-Hut).

Each school 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 these should be turned off and unplugged as well
- Computers should be moved away from windows, off the floor and covered with plastic if possible. (If a physical emergency/threat……flood, earthquake, etc.)

6.2 Cyber Attacks/Security Incident Preventions

- Backup data regularly, and verify the integrity of those backups and test the restoration process to ensure it is working
- Secure backups: Ensure that all backups are not connected permanently to the computers and networks they are backing up. For example, secure backups in the cloud or physically store backup data offline and off campus.

7. Test Disaster Recovery Plan (TDRP) Exercising

It is good practice to hold test exercises at the beginning of each school year to assure all members of the ERT know their responsibilities in the event of a disaster. Plan exercising ensures that emergency teams are familiar with their assignments and, more importantly, are confident in their capabilities.

Appendix A- Technology Disaster Recovery Plan (TDRP) for KSD Technology Equipment (Removed for online security reasons-see hard copy)

8. KSD Technology Outline and Procedures

Overview

The Kimberly School District's intention for publishing Policies and Procedures is to provide clear guidelines and expectations aligned with District's established mission of providing users with the best resources possible to educate every student. KSD is committed to protecting users from illegal or damaging actions by individuals, either knowingly or unknowingly. Network related systems, including but not limited to computer equipment, software, operating systems, storage media, mobile devices, network accounts providing electronic mail and or resources, WWW browsing, and file transfer services are the property of KSD. These systems are to be used for educational and school business-related purposes with the intent of serving the interests of the students, teachers, and other staff members of KSD. Maintaining a network requires proper planning, organization, monitoring, and effective security. A team effort involving the participation and support of every KSD employee and affiliate is required to meet and exceed the standards set forth by Idaho State Law, Federal Law, the Kimberly School District Board of Trustees and KSD Administrators. It is the responsibility of every computer user to know these guidelines, and to govern themselves accordingly.

Purpose

The purpose of the following procedures is to outline the acceptable use of the network-related systems within KSD. These rules are in place to protect the students, staff, and the district. Inappropriate use, improper planning, and disregard of these procedures exposes KSD to risks including compromise of network systems and services, possible damage to the network, and legal issues.

Scope

These procedures apply to students, employees, contractors, consultants, temporary employees, authorized guests, substitute teachers and other workers at KSD including all personnel affiliated with third parties. This also applies to all equipment that is owned or leased by KSD to include all future purchases. (See KSD 3612 Policy)

8.1 Acceptable Use of Electronic Networks Procedure (KSD 3612 P)

All use of electronic networks shall be consistent with the District's goal of promoting educational excellence by facilitating resource sharing, innovation, and communication. These procedures do not attempt to state all required or proscribed behaviors by users. However, some specific examples are provided. The failure of any user to follow these

procedures will result in the loss of privileges, disciplinary action, and/or appropriate legal action.

Terms and Conditions

1. **Acceptable Use** – Access to the District's electronic networks must be:
    - For the purpose for education or research and consistent with the educational objectives of the District; or
    - For legitimate business use.

2. **Privileges** – The use of the District's electronic networks is a privilege, not a right, and inappropriate use will result in a cancellation of those privileges. The system administrator (and/or building principal) will make all decisions regarding whether or not a user has violated these procedures, and may deny, revoke, or suspend access at any time. His or her decision is final.

3. **Unacceptable Use** – The user is responsible for his or her actions and activities involving the network. Some examples of unacceptable uses are:

    - Using the network for any illegal activity, including violation of copyright or other contracts, or transmitting any material in violation of any U.S. or state law:
    - Unauthorized downloading of software, regardless of whether it is copyrighted or de-virused;
    - Downloading copyrighted material for other than personal use;
    - Using the network for private financial or commercial gain;
    - Wastefully using resources, such as file space;
    - Hacking or gaining unauthorized access to files, resources, entities;
    - Invading the privacy of individuals, which includes the unauthorized disclosure, dissemination, and use of information of a personal nature about anyone;
    - Using another user's account or password;
    - Posting material authored or created by another, without his/her consent;
    - Posting anonymous messages;
    - Using the network for commercial or private advertising;
    - Accessing, submitting, posting, publishing, or displaying any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, harassing, or illegal material; and
    - Using the network while access privileges are suspended or revoked.

4. **Network Etiquette** – The user is expected to abide by the generally accepted rules of network etiquette. These include, but are not limited to, the following:

    - Be polite. Do not become abusive in messages to others.
    - Use appropriate language. Do not swear or use vulgarities or any other inappropriate language.
    - Do not reveal personal information, including the addresses or telephone

numbers, of students or colleagues.

- Recognize that electronic mail (e-mail) is not private. People who operate the system have access to all mail. Messages relating to or in support of illegal activities may be reported to the authorities.
- Do not use the network in any way that would disrupt its use by other users.
- Consider all communications and information accessible via the network to be private property.

No Warranties – The District makes no warranties of any kind, whether expressed or implied, for the service it is providing. The District will not be responsible for any damages the user suffers. This includes loss of data resulting from delays, non-deliveries, missed deliveries, or service interruptions caused by its negligence or the user's errors or omissions. Use of any information obtained via the internet is at the user's own risk. The District specifically denies any responsibility for the accuracy or quality of information obtained through its services.

Indemnification – The user agrees to indemnify the District for any losses, costs, or damages, including reasonable attorney fees, incurred by the District, relating to or arising out of any violation of these procedures.

Security – Network security is a high priority. If the user can identify a security problem on the internet, the user must notify the system administrator or building principal. Do not demonstrate the problem to other users. Account information and passwords are confidential. **KSD employees are required to change their system password every 90 days.** Users are not to use another individual's account without written permission from that individual. Attempts to log on to the internet as a system administrator will result in cancellation of user privileges. Any user identified as a security risk may be denied access to the network.

Vandalism – Vandalism will result in cancellation of privileges, and other disciplinary action. Vandalism is defined as any malicious attempt to harm or destroy data of another user, the internet, or any other network. This includes, but is not limited to, the uploading or creation of computer viruses.

Telephone Charges – The District assumes no responsibility for any unauthorized charges or fees, including telephone charges, long-distance charges, per-minute surcharges, and/or equipment or line costs.

Copyright Web Publishing Rules – Copyright law and District policy prohibit the republishing of text or graphics found on the Web or on District websites or file servers, without explicit written permission.

- For each re-publication (on a Website or file server) of a graphic or text file that was produced externally, there must be a notice at the bottom of the page crediting the original producer and noting how and when permission

was granted. If possible, the notice should also include the Web address of the original source.

- Students and staff engaged in producing Web pages must provide library media specialists with e-mail or hard copy permissions before the Web pages are published. Printed evidence of the status of "public domain" documents must be provided.
- The absence of a copyright notice may not be interpreted as permission to copy the materials. Only the copyright owner may provide the permission. The manager of the Website displaying the material may not be considered a source of permission.
- The "fair use" rules governing student reports in classrooms are less stringent.
- Student work may only be published if there is written permission form both the parent/guardian and the student.

Use of Electronic Mail

- The District's electronic mail system is managed by the District. The District provides e-mail to aid students and staff members in fulfilling their duties and responsibilities and as an educational tool.
- The District reserves the right to access and disclose the contents of any account on its system, without prior notice or permission from the account's user. Unauthorized access by any student or staff member to an electronic mail account is strictly prohibited.
- Each person should use the same degree of care in drafting an electronic mail.
- Electronic messages sent through the district provided services are considered property of KSD. Such messages reflect on the name and reputation of the district. Users will be held personally responsible for the content of any and all electronic messages transmitted to both internal and external recipients.
- Any message received from an unknown sender via the internet should be verified as to the message's authenticity and the nature of the file so transmitted.
- Use of the District's electronic mail system constitutes consent to these regulations.

Internet Safety and Privacy

- Internet access is limited to only those "acceptable uses", as detailed in these procedures. Internet safety is almost assured if users will not engage in "unacceptable uses", as detailed in these procedures, and will otherwise follow these procedures.
- Staff members shall supervise students while students are using District internet access, to ensure that the students abide by the Terms and Conditions for internet access, as contained in these procedures.

- **Confidentiality of Student Information (taken from ISBA 3270-6)**
  (would like to add this to our procedures and policy)

  Personally identifiable information concerning students may not be disclosed or used in any way on the internet without the permission of a parent or guardian and the student or, if the student is 18 or over, the permission of the student. Students should be aware that conduct on the District's computer or using the District's server may be subject to public disclosure depending upon the nature of the communication. Users should never give out private or confidential information about themselves or others on the internet, particularly credit card numbers and social security numbers.

- Each District computer with internet access has a filtering device that blocks entry to visual depictions that are: a) obscene, b) pornographic, or c) harmful or inappropriate for students, as defined by the Children's Internet Protection Act and as determined by the Superintendent or designee.
- The system administrator and building principals shall monitor student internet access.

Legal Reference: Children's Internet Protection Act, P.L. 106-55420 U.S.C. §6801, et seq.47 U.S.C. §254(h) and (l).

9.0 Technology Department Administration & Technician Responsibilities

It is the responsibility of the KSD Technology Dept. Technicians (Network Manager, Helpdesk Specialist, and/or Technology Secretary) to follow the guidelines and policies of the district, state and federal laws.

Technicians work with the Technology Supervisor. Training and meetings, as determined by the Technology Supervisor, are to be held between the KSD Technicians and the Technology Supervisor in order to maintain close working relationships and openness in day-to-day communications.

Among their other responsibilities, the KSD Technicians should use reasonable efforts to:

- Respond to requests for support, information, problem determination and problem resolution.
- Become familiar with all applicable KSD Technology policies.
- Participate in required Technicians trainings and regular meetings as determined by the Technology Supervisor.
- Take precautions against theft of or damage to the system components and information.
- Comply with terms of all hardware and software licensing agreements applicable to the system.

- Treat information about, and information stored by, the network users in an appropriate manner and to take precautions protecting the security of the network and the security and confidentiality of the information contained therein.
- Promptly inform the Technology Supervisor of any computing incidents which clearly compromise network integrity, including but not limited to:

    - Notification by outside institutions or individuals of any incident.
    - Data loss or theft
    - Inappropriate systems or information access or use
    - Any other breach or violation of KSD Technology Policies of which they become aware.
    - Promptly notify the Technology Supervisor of material changes in network architecture or administration.

KSD Technicians, when requested, are expected to cooperate fully with District Administration in any investigation, identification, and resolution of network incidents. KSD Technicians are not responsible for the content of files, images, video or audio clips, electronic communications, and news postings produced by others. The KSD Technicians are also not responsible for unauthorized software installed by others. KSD Technicians are responsible, however, for notifying the Technology Supervisor of any observed violations of KSD District policies, licensing agreements with software manufacturers, or observed violations of local, state, or federal laws regarding these matters.

10.0 Purchasing

The KSD Technology Department is responsible for the seamless integration of any hardware or software into the existing network system. While software will be approved and can be purchased (or awarded through grants) by department and building administrators, it is recommended that the KSD technology department be notified prior to purchase to ensure compatibility with current district technology whenever possible.

11.0 Disposal of Technology Equipment

All technology equipment must be disposed of in a manner that adheres to all State and Federal Laws as well as KSD School Board Policy.

12.0 Enforcement

Failure to adhere to these policies and guidelines may result in suspension or revocation of the offender's privilege or access to the network and/or other disciplinary or legal action.

13.0 Revisions

The KSD 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.

Board Approved:_____