Austin Public Schools

ENGAGING AND EMPOWERING
ALL LEARNERS FOR LIFE!

Technology Disaster Recovery Plan

Austin Public School
Independent School District 492
401 Third Avenue NW
Austin, MN 55912
(507) 460-1900
www.austin.k12.mn.us

(This page left blank intentionally)

Independent School District 492
Technology Services Disaster Recovery Plan

Last Revision October 08, 2015

!! Confidential Items Have Been Removed!!

Emergency Telephone Numbers (911)

Contact Type	Institution / Title	Contact Person	Office Phone
Emergency	Austin Fire Dept	Jim McCoy	507-433-3405
Emergency	Austin Police Dept.	Brian Krueger	507-433-9400
Emergency	Mower County Sherriff	Teresa Amazi	507-437-9700
Police Liaison	Austin Police Dept.	James Lunt	507-460-1809
Police Liaison	Austin Police Dept.	Kevin Sederquest	507-460-1509
Ambulance Service	Gold Cross	-----	507-433-1850
Medical Service	Mayo Health System	-----	507-433-7351
Emergency Mgmt.	Statewide Metro	----- -----	800-422-0798 651-291-6780
ISD492 Contact	Superintendent	David Krenz	507-460-1900
ISD492 Contact	Director of HR	Brad Bergstrom	507-460-1904
ISD492 Contact	Director of Finance	Mark Stotts	507-460-1913
ISD492 Contact	Director of Facilities	Mat Miller	507-460-1929
ISD492 Contact	Director of IT	Burke Egner	507-460-1933
Austin Utilities	General Manager	Mark Nibauer	507-433-8886
Austin Utilities	Electric Dist. Director	Tom Tylutki	507-433-8886
Phone Vendor	Jaguar Communications	Mike Wilker	507-214-0259
Internet Provider	Jaguar Communications	Mike Wilker	507-214-0259
Cable Provider	Charter Communication	Dan Schiltz	763-241-4152
Security/Fire Systems	UHL Company	Mike Polley	763-657-2654

1. Possible Disaster Scenarios and Personnel Notification Chart

Note: In case of fire or life threatening emergency situations, take immediate action by sounding appropriate alarms and calling 911 before proceeding.

This chart is divided into 3 sections. A. Primary Contacts B. Secondary Contacts C. Vendor Contacts

1. Primary contacts shall be notified first.
2. Primary contacts will notify secondary contacts if the situation warrants it.
3. Primary contacts will contact vendors to assist in recovery operations; as required.

Event	Name	Role
Primary Contacts		
Technology Equipment Failure or Data Loss of Network Services	Burke Egner Tony Campbell	Director of IT Network Administrator
Environmental equipment failure natural disaster / ice, wind, fire or water damage	Mat Miller	Director of Facilities
Secondary Contacts		
The Superintendent shall be notified of any situation that has impact beyond a particular building/ program, affects safety, or requires police intervention.	David Krenz	Superintendent
The Director of Human Resources shall assume the role and responsibility if the Superintendent is unavailable during a crisis situation.	Brad Bergstrom	Human Resources

2. Introduction:

This document comprises the Information Technology Department disaster recovery plan for Independent School District 492, Austin Public Schools, 401 3rd Ave. NW Austin, MN. The information present in this plan guides district management and technical staff in the recovery of computing and network facilities operated by the district, in the event that a disaster destroys all or part of the facilities, equipment, or data. Although this disaster recovery plan currently focuses on recovery of the technology systems in use by the district, this plan is not exclusive of the district's comprehensive emergency procedures plan, but is rather designed to be an integral component of the district's comprehensive emergency procedures plan.

IN AN EFFORT TO AVOID UNNECESSARY AND CONFUSING DUPLICATION OF DOCUMENTATION, THIS DOCUMENT WILL SOMETIMES REFERENCE KEY INFORMATION CONTAINED IN THE DISTRICT'S EMERGENCY PROCEDURES MANUAL.

3. Distribution:

Two versions of this document will be created, a public version and a confidential version.

3.1 Public

One copy will marked with Public in the title and stored in the district's secured intranet site in HTML format as a web document and in PDF format for download. The public version will include general information.

3.2 Confidential

The confidential copies of this document will be marked "Confidential, Not For Distribution". These copies are not intended for district wide publication. One confidential copy will be kept with the Administrative Assistant to the Superintendent. One copy will be kept in the Technology Services safety deposit box located at Sterling State Bank in Austin, MN. The confidential version is designed to facilitate working with the vendors and insurance company in the event of a disaster. The confidential version will include sensitive information such as: vendor Contact Numbers; Warranty and Support Contract Numbers and General Information; Software License Numbers; Equipment Inventories.

4. Description:

The primary reason for the development of this disaster recovery plan is to ensure the ability of the district to function as effectively as possible in the event of a severe disruption to normal operations. Severe disruptions can arise from several sources: natural disasters (tornadoes, fire, flood, etc.), equipment failures, process failures, from mistakes or errors in judgment, as well as from malicious acts (such as denial of service attacks, hacking, viruses, and arson, among others). While the district may not be able to prevent any of these disruptions from occurring, disaster recovery planning will enable the district to resume essential operations more rapidly than if no plan existed. Before proceeding further, it is important to distinguish between Loss Prevention Planning and Disaster Recovery Planning. The focus of loss prevention planning is on minimizing the districts exposure to risks that can threaten normal operations. In the technology realm, loss prevention planning includes such activities as providing for system back-ups, making sure that passwords remain confidential, that desktops are locked when unattended, that perimeter security is in place, and operating systems remain secure and free of viruses and spyware. Disaster recovery planning focuses on the set of actions the district must take to restore service and normal operations, or as nearly normal as possible given the constraints of fiscal responsibility, in the event that a significant loss has occurred for critical functions. A systematic disaster recovery plan looks for the common elements in any disaster: i.e., loss of information, loss of personnel, loss of equipment, loss of access to information and facilities, and seeks to design a contingency program that encompasses all the critical district systems. This plan will specify the set of actions for implementation for each activity in the event of any of these disruptions in order for the unit to resume doing business in the minimum amount of time. The primary focus of this document is on disaster recovery of technology services.

5. Objectives:

The overall objectives of the district's Technology Disaster Recovery Plan (TDRP) are;

- Identify the district's critical systems, applications, and data.
- Identify and categorize risk.
- Create contingencies to mitigate the impact of identified and unidentified risk.
- Protect the district's critical records from data loss and corruption.
- Protect district resources and employees.
- Protect the district's reputation and integrity.
- Ensure the district is able to function effectively during the disaster recovery stage.
- Recover data and information.
- Restore operations as quickly as possible.

6. Assumptions:

Certain types of organizations, such as financial institutions, cannot function without the computers they need to stay in business. Their recovery plans usually focus on quick recovery, or even zero down time, through duplication and synchronization of redundant server systems in separate facilities. Unfortunately; this is the most expensive form of fault tolerance because this strategy requires physical and logical duplication of equipment, operating systems, software, and data. Special software is also required to keep the redundant sites synchronized. Utilizing this kind of fault tolerant strategy would increase the technology budget by over 150%. Obviously; the district is forced to make compromises between the amount of time, effort, and money that can be spent in planning and preparation for a disaster, and the amount of data loss and downtime that can be tolerated during systems recovery following a disaster. The district planning committee has made a determination that to be fiscally responsible, the district will accept some measure of risk and downtime in return for having the option to use insurance proceeds to rebuild the network systems after a disaster. Recovery efforts outlined in this plan are designed to restore network system operations as soon as possible, and to restore data as completely as possible. It is recognized that significant effort will be required to restore the district data to the state it was in before the disaster, and that some data may be lost. The following statements reflect the compromises and risks that were assumed because of the fiscal realities imposed by budget constraints.

- In the case that the 3rd floor server room at Austin High Schools was totally destroyed, the district is assuming the risk that up to 31 days of data could be lost.

- In the event that the citywide fiber optic network is totally destroyed, the district is assuming the risk that no inter-site (school to school) network communication may be available for up to 21 days.

- In the case of a disaster, the district can function without critical services for up to 2 business days.

- In the case of a disaster, the district can function without essential services for up to 7 business days.

- In the case of a disaster, the district can function without desirable services for more than 7 business days.

- Normally available staff members may be rendered unavailable by a disaster or its aftermath, or may be otherwise unable to participate in the recovery.

- Recovery of a critical subset (recovery workload) of the unit's critical functions and applications systems during the recovery period will allow the unit to continue critical operations adequately.

- Each department will have a plan on how to operate until information network services are restored within the acceptable parameters described above.

7. Criteria for invoking the plan

7.1 Follow the emergency procedures manual.

7.1.1 In the event that a disruption of service is caused by a life threatening emergency situation, or by a serious mechanical failure, the immediate situation should be dealt with according to the processes described in the appropriate section of the districts emergency procedures manual.

7.1.2 The technology disaster recovery plan will not be implemented until the sites have been secured and all threats to life and personal injury have been mitigated.

7.2 Discovery:

7.2.1 In the event that an employee discovers that network services are unavailable, they should contact network services.

7.2.2 In the event that an employee discovers an emergency situation, the employee should notify their immediate supervisor or refer to page 9 of the districts emergency procedures manual; and notify one of the persons listed therein.

7.3 Determination:

7.3.1 The network coordinator or their alternate shall determine whether a given event meets the definition of a technology disruption event.

7.3.2 In the event that the network coordinator and/or their alternate is unavailable or incapacitated, those persons listed as key decision makers on page 9 of the district emergency procedures manual shall determine whether a given event meets the definition of a disaster emergency.

7.3.3 In the event that a disaster emergency is declared, the appropriate actions will be executed as outlined in the districts emergency procedures manual.

Notification Procedures:

8.1 Natural Disaster, Environmental, or Mechanical Causes:

8.1.1 Once emergency personnel and supervisors have been notified, the buildings and grounds director and/or building supervisor should be notified.

8.1.2 The buildings and grounds director, principal or building supervisor should notify the Director of Information Technology.

8.2 Human or Technological Causes:

8.2.1 If there is a disruption of service due to virus infection, software failure, security breach, malicious destruction of data, accidental loss of data, or for an unknown reason, the Director of Information Technology should be notified immediately.

8.2.2 The Director of Information Technology will notify the superintendent.

8.2.3 The Superintendent and Director of Information Technology will make additional notifications outlined in the districts emergency procedures manual if necessary.

8.3 Communication

8.3.1 The Superintendent shall be notified of any situation that has impact beyond a particular building/program.

8.3.2 The Superintendent shall be notified in the following situations:

8.3.2.1. Police intervention with an employee or outsider

8.3.2.2. Safety concerns for students or staff

8.3.2.3. Major disruption of building or program operation

8.3.3 Contact with the Superintendent initiates the following guidelines:

8.3.3.1. Communication originates with the Superintendent and flows directly to Principals/Supervisors.

8.3.3.2. Action decisions are taken after consultation with the Superintendent unless an autonomous decision is needed to resolve an immediate emergency.

8.3.4 The district crisis team will meet as soon as possible at the onset of a crisis situation.

8.3.5 The Director of Human Resources shall assume the role and responsibility if the Superintendent is unavailable during a crisis situation.

Roles Responsibilities and Authority

9.1 Key decision makers.

- Superintendent
- Director of Finance and Operations
- Director of Human Resources

9.2 Damage Assessment Team

- Director of Buildings and Grounds
- Director of Information Technology
- Building Principals

9.3 District Recovery Team Managers

- Superintendent
- Director of Finance and Operations
- Director of Human Resources
- Director of Buildings and Grounds
- Director of Information Technology

Refer to the district emergency procedures manual for the names and contact information of the individuals who hold these positions.

10. Risk Assessment – Data Loss:

Categories of identified risk that could result in data loss listed in order of most likely occurrence.

10.1 High Probability:

- ✓ Equipment Failure
- ✓ Accidental Destruction of Data
- ✓ Malicious Destruction of Data by Personnel or Students Originating From Within The School District.
- ✓ Tornado – Severe Thunderstorm (Physical Destruction or Water Damage)
- ✓ Fire in Server Room

10.2 Medium Probability:

- ✓ Malicious Destruction of Data by External Attack Originating from outside the School District. (Hacker - Viruses)
- ✓ Water Damage Due To Accidental Activation Of Sprinkler System
- ✓ Failure to Maintain Correct Environmental Operating Temperature in Server Rooms and Equipment Closets.
- ✓ Fire At Locations Other Than AHS

10.3 Low Probability:

- ✓ Ice Storm
- ✓ Damage to Fiber Optic Lines
- ✓ Fire in Equipment Closets (All Locations)

11. Risk Assessment – Network Disruption:

Categories of identified risk that could result in a network disruption listed in order of most likely occurrence.

11.1 High Probability:

- ✓ Equipment Failure (Items Listed In Section 10)
- ✓ Power Outage
- ✓ Accidental Destruction of Fiber Optic Lines
- ✓ Ice or Wind Storm

11.2 Medium Probability:

- ✓ Virus Infection, Malicious Code, or Denial Of Service Attack Originating From Inside The Network Perimeter.
- ✓ Water Damage Due To Accidental Activation Of Sprinkler System
- ✓ Extreme Environmental Operating Temperatures in Server Rooms And Equipment Closets.
- ✓ Intentional Destruction of Physical Equipment By Personnel Or Students Originating From Within The School District.

11.3 Low Probability:

- ✓ Virus Infection, Malicious Code, or Denial of Service Attack Originating From Outside The Network Perimeter.
- ✓ Fire
- ✓ Intentional Destruction of Physical Equipment by Persons Originating from Outside the School District.

12. Risk Assessment – District Programs

12.1 Critical:

The district cannot conduct business without these programs and services:

Program	Maximum Downtime in Days	Data Loss Tolerance POR – Point of Recovery in Days
Skyward	2	31
Infinite Campus (SIS)	2	1
E-Mail	2	NA Data is stored on remote server
SpedForms	2	31
File Server	2	31
Viewpoint Data Warehouse	2	31
SharePoint (Website)	2	31

12.2 Essential:

The district can conduct business without these programs and services for a limited time by using manual methods to conduct business and record data. Manually entered and recorded data will be incorporated into recovered systems.

Program	Maximum Downtime in Days	Data Loss Tolerance POR – Point of Recovery in Days
Horizon	7	31
Destiny	7	31
HVAC Control System	7	NA Data is stored on individual panels in each building.
Work Order System	7	NA Data is stored on remote server
Scantron Performance Series	7	NA Data is stored on remote server
Read180	7	7

12.3 Necessary:

The district can conduct business without these programs and services for an indefinite period of time by using manual methods to conduct business and record data. Manually entered and recorded data will be incorporated into recovered systems.

Program	Maximum Downtime in Days	Data Loss Tolerance POR – Point of Recovery in Days
Protec – DSX Security Doors	7	NA Data is stored on individual panels in each building.
DIBELS Data System	7	NA Data is stored on remote server
Naviance Succeed	7	NA Data is stored on remote server
Textbook Solutions	7	NA Data is stored on remote server
ClarityNet	7	NA Data is stored on remote server
Raz-Kids Reading Program	7	NA Data is stored on remote server

13. Data Backup Procedures:

The data for the following programs will be archived as described in this table. Automated backup procedures will be audited once per week at a minimum. Only services hosted On-Site are listed.

Program	POR from 12.1	Daily On-site	Daily Off-site	Weekly On-site	Weekly Off-site	Month Off-site	Annual Off-site
Skyward	31	Yes	**No**	Yes	**No**	Yes	Yes
Infinite Campus (SIS)	1	**No**	Yes	**No**	Yes	Yes	Yes
File Server	31	Yes	**No**	Yes	**No**	Yes	Yes
SharePoint (Website)	31	Yes	**No**	Yes	**No**	Yes	Yes
Horizon	31	Yes	**No**	Yes	**No**	Yes	Yes
Destiny	31	Yes	**No**	Yes	**No**	Yes	Yes
Read180	7	Yes	**No**	Yes	Yes	Yes	Yes

14. Estimated Downtime From Single Points Of Failure:

Failure of the following listed equipment will disrupt most services for the entire district.

14.1 Redundant Cisco 6500 Estimated Maximum Downtime Hours: 48

In the event of a complete dual failure there will be no network traffic between schools and between classrooms at the high school.

14.2 Servers Estimated Maximum Downtime Hours: 48

In the event of a failure the service associated with the failed server will not be available, excluding e-mail which is clustered.

14.3 Array Estimated Maximum Downtime Hours: 48

In the event of a failure no data will be available and almost all services will not be available, internet will continue to function.

14.4 Jaguar Estimated Maximum Downtime Hours: 24

In the event of a failure no internet service will be available.

Important!!

There are 2 spare Ethernet to Fiber transceivers stored with Jaguar Communications for use in cases of equipment failure.

14.5 Fiber Estimated Maximum Downtime Hours: 24

The fiber optic network was designed to be as redundant as possible with 2 independent links connecting each site.

There are 3 locations where this wasn't possible due to physical or budget limitations. These locations are; IJ Holton, Ellis Middle school, Athletic Field.
In the event that the fiber optic cable is damaged in one of these locations all no data, network services, or internet will be available.

14.6 **Phone Service Estimated Maximum Downtime Hours: 24**

Important!!

In the event of a network failure phone service will be unavailable.
At least one independent analog telephone line exists at each location with the exception of Wescott Field for use in case of an emergency during a network outage.

15. Recovery Procedures

This section describes the most common anticipated network disruptions and the steps that should be followed to recover from them. (See sections 10 and 11) These recovery procedures should be implemented by the Information Technology Department once a determination of the problem has been made and appropriate decision makers have been notified. (See section 8)

Important!!

The recovery procedures listed herein are based upon the assumption that each department has created a disaster operations plan which details how operations will be conducted without the support of the network information system for the periods specified in section 12.

15.1 Core or Edge Switch Failure

Once it has been determined that there is a disruption in network service due to a switch failure the following actions should be taken.

15.1.1 Call Cisco Technical Assistance Center – TAC and open a case with them.
15.1.2 Contract numbers, serial numbers, and general switch information can be found in the contract information appendices.

15.2 Think Server, SAN Array, HBA, Or SP Failure.

Once it has been determined that there is a disruption in network service due to a SAN related failure the following actions should be taken.

15.2.1 Call Lenovo and/or IBM Support and open a case with them.
15.2.2 Contract numbers, serial numbers, and general switch information can be found in the contract information appendices.

15.3 Power Outage

15.3.1 Notify the Director of Buildings and Grounds. The contact number can be found in the Emergency Numbers section.

15.4 Extreme Temperatures Found In Equipment Rooms Or Closets.

15.4.1 Notify the Director of Buildings and Grounds. The contact number can be found in the Emergency Numbers section.

15.5 Water Damage Found In Equipment Rooms Or Closets.

15.5.1 Notify the Director of Buildings and Grounds. The contact number can be found in the Emergency Numbers section.

15.6 Destruction Of Physical Equipment By Personnel Or Students Originating From Within The School District.

15.6.1 Notify the Director of Buildings and Grounds.

15.6.2 Notify Superintendent or Human Resource Director.

15.6.3 Notify Police Liaison and/or Police Department if applicable. The contact number can be found in the Emergency Numbers section.

15.7 Fiber Optic Cable Break Once it has been determined that there is a disruption in network service due to a fiber optic cable break the following actions should be taken.

15.7.1 Shutdown the switch ports associated with the cable break.

15.7.2 Call the Austin Public Utilities contact listed in section 1 and provide notice to them including as much detail as possible.

15.7.3 Once the repair has been made bring the switch ports back online and test all affected systems.

15.8 Fire, Tornado, or Severe thunderstorm resulting in complete loss of AHS 3rd floor Server Room.

15.8.1 Notify damage assessment team as listed in section 9.

15.8.2 Damage assessment team will work with district recovery team to determine best course of action.

15.8.3 Decision will be made regarding use of an emergency operations center.

15.8.4 Equipment vendors and utility contractors will be contacted for bids on replacement equipment and construction as needed. See section 1.

15.8.5 Insurance company will be notified that a loss has occurred.

15.8.6 Equipment inventories and financial records will be used to document loss.

15.8.7 If emergency operations center will be used, work with vendors and contractors to deploy and configure necessary equipment.

15.8.8 Replay data from most recent backup and test systems.