

**District Planning Guide**
April 20, 2016

This Planning Guide is a high-level checklist intended to assist Kentucky’s public schools create effective disaster recovery plans.

Disaster Recovery v2.1

Table of Contents

[PROACTIVE STEPS – DO THESE BEFORE A DISASTER HAPPENS 2](#_Toc451413316)

[STEP 1: Document Names and Contact Information for All Roles 2](#_Toc451413317)

[STEP 2: Define Severity Levels Addressed by the Recovery Plan 3](#_Toc451413318)

[STEP 3: Define Critical Technology Assets 3](#_Toc451413319)

[STEP 4: Identify Alternate Site(s) 4](#_Toc451413320)

[STEP 5: Define Storage and Maintenance of the Disaster Recovery Plan 5](#_Toc451413321)

[STEP 6: Testing and Validation 5](#_Toc451413322)

[REACTIVE STEPS –DISASTER RECOVERY 6](#_Toc451413323)

[STEP 1: Implementation of the Plan 6](#_Toc451413324)

 NOTE: The following recommendations are built upon experiences gained from industry and actual efforts required in the Commonwealth. Even so, they may not address all environments and every situation found in Kentucky’s schools and districts. This guide should be used as an outline to assist districts in planning and implementing their own Disaster Recovery Guides. Additional guides, plans and articles can be found online and may provide additional important assistance.

# PROACTIVE STEPS – DO THESE BEFORE A DISASTER HAPPENS

## STEP 1: Document Names and Contact Information for All Roles

1. Define Who is in Charge of Recovery Effort
	1. Assesses the situation and declares/confirms a disaster, or crisis
	2. May lead recovery effort, or delegate to others
	3. Provides single point of contact for recovery effort
2. Define a Technical Recovery Lead (HW, SW, systems, facilities, etc.)
	1. Contacting stakeholders to inform and request action
		1. Vendors such as Dell, Tyler Tech., local power, phone, etc.
	2. Getting systems back on line via backups
	3. Coordinate with Business Recovery Lead
	4. Updates DR Plan
3. Define a Business Recovery Lead (Legal, processes, communications, etc.)
	1. Contacting stakeholders
		1. Insurance
		2. The Media
		3. Emergency Medical Technicians
	2. Coordinate with Technical Recovery Lead (may be same person)
	3. Updates DR Plan
4. Document All Key Partners
	1. Systems & Service Vendors
		1. Local fiber vendor
		2. Electrician
		3. Low voltage wiring vendor
		4. HVAC
		5. Network vendor
		6. Telecom vendor
	2. District Leadership
		1. Superintendent
		2. Board members
		3. CIO
		4. Tech staff
		5. Facilities staff
		6. Emergency Purchases staff
	3. KDE Leadership
		1. KETS Engineer
		2. KIDS Office
		3. KETS Service Desk
	4. Other
		1. EMT Services
		2. Insurance
		3. Local Media (newspaper/radio)
		4. Parents/Legal Guardians
5. Define Subordinate and Backup Leads, as necessary, for Individual Process and Systems
6. Establish a communications plan
	1. Define availability and accessibility expectations
	2. Discuss escalation paths
	3. Define list of first calls to be made (e.g. Emergency/911, district leadership, parents/legal guardians, KDE staff and Service Desk, utilities, insurance, vendor partners)

## STEP 2: Define Severity Levels Addressed by the Recovery Plan

1. Define and make clear the severity level(s) and identifying characteristic(s). Will the DR Plan address each? Just one? Why this and not that? Examples:
	1. Disaster - Catastrophic loss of hub site and all systems & assets contained therein. Everything, or nearly everything, is gone. No services are available.
	2. Crisis – Partial loss of hub site systems & assets. One or more critical services are down.
	3. Emergency – One or more critical services are experiencing problems. Physical loss of ingress / egress access to hub site.

## STEP 3: Define Critical Technology Assets

1. Inventory your systems
	1. Critical District Systems (onsite or cloud)
		1. Food Service
		2. Library
		3. File Storage
		4. Bus/Transportation
		5. Telephone/Voice/Video
		6. District Website
		7. Secure Web Gateway, etc.
	2. Critical Network Hardware
		1. Layer 3 Switch/Core routers
		2. Uninterruptable Power Supplies
		3. Include a network Topology Diagram with plan for rerouting the district fiber network to support move of the hub site to another physical location.
	3. Critical Business Continuity Hardware
		1. Check printers, scanners, phones, etc.
	4. Software, especially mission critical applications.
		1. Do you have physical copies for reinstall? Are they latest version? Will you require Internet access to reinstall? Do you have license keys? Are cloud versions available?
	5. Inventory Information/data. Note the critical information required to conduct business. Critical data SHOULD be located within systems also identified and known as critical. Are they?
2. Define the business/recovery priority of each system (1, 2, or 3) along with an expected “time for recovery” so that the most important will be recovered first and there is an accurate expectation of time required for recovery.
	1. Include existing disaster recovery or business continuity plans provided by vendor partners for each system (onsite or cloud)
	2. Define the number of days business can be conducted without each of these systems. You may find several redundant systems
	3. Assign each system a realistic estimate of days to restore, and notify business stakeholders of this timeframe, in order to set their expectations.
	4. Inventory System Data Back-ups
		1. What’s backed-up?
			1. Everything?
			2. Only Critical information?
			3. Some of the Critical Information?
		2. Backup storage location
		3. Steps to restore from backups
3. Inventory Workstations and peripherals
4. Inventory Privileged Accounts and passwords
	1. What is the purpose of each account?
	2. To which system(s) does each account have access?
	3. Are the passwords to each system account accessible and stored securely?
5. Request each vendor to provide a statement regarding their abilities and responsibilities to you in the event of a disaster, both for setting up new services at a recovery location and restoring services at the original location
	1. Utilities (water, electric, HVAC - who is your point person and when can I expect services?)
	2. Computer providers (how fast can replacements be on the ground?)
		1. Will they be ready to join our domain?
	3. Software/Critical Application companies (how fast…?)

## STEP 4: Identify Alternate Site(s)

1. Identify primary Emergency Operations Center (EOC)/alternate site and potential alternate location, just in case. Select a site based on necessary recovery window and available resources, which will impact the shortest path to restore services. Are there existing resources available, e.g. trailers, mobile classrooms? Rent from a vendor? Location in neighboring district?
	1. Does the proposed site already have the following?
		1. Power
		2. Lighting
		3. Network
		4. Phones
		5. Office Supplies (Pens/Paper/Whiteboard/Markers/Coffee/etc.)
		6. Water/restroom facilities
	2. Is it close enough to be accessible by staff, but far enough away to not be impacted by the same disaster?
		1. Different weather systems (e.g. floods, tornados)
		2. Different electric grid
		3. Accessible by main roads
	3. Identify travel and accommodation arrangements for critical technology and business continuity staff

## STEP 5: Define Storage and Maintenance of the Disaster Recovery Plan

1. Keep the DR Plan, including all inventories and associated documents, offsite, secure, and accessible (cloud, flashdrive around neck, etc., all of the above) to key staff. Consider keeping hardcopies available somewhere, as well, in case there is a larger outage that prevents internet access citywide.
	1. Plan should be reviewed and updated at least annually, or after significant events such as key staff changes or a disaster, where lessons learned can inform plan updates.

## STEP 6: Testing and Validation

1. Having a disaster recovery plan is just the first, very important, step. The plan should be tested whenever substantial changes in infrastructure or staff occur.
	1. Verbal or Checklist Test – Like a dress rehearsal, this style of test brings everyone together to run through the defined recovery steps, without the risk of actually turning any systems off to test. This rehearsal can help everyone see the big recovery picture and highlight problems or missing jobs.
	2. Simulation Test – After the checklist test, the next step is to simulate a disaster. There are various levels of simulation testing, from no impact on existing services to actually stopping existing services to see if they can be successfully recovered. There is some amount of risk involved with these tests, so ensure all affected parties are informed and engaged and then proceed with caution.

# REACTIVE STEPS –DISASTER RECOVERY

## STEP 1: Implementation of the Plan

1. Assess the extent of the loss of critical district technology assets
	1. Partial loss including… (begin with priority items)
	2. Total loss
2. Contact key staff and partners as defined in plan
3. Move control and operations teams to EOC/Alternate Site. If need be, address the following issues before moving:
	1. Facility space appropriated
	2. Physical security ensured
	3. Utilities are hooked up and available
	4. Environmental and comfort controls in place and functioning
4. Set communication plan in motion
5. Begin recovery of critical business systems
	1. Check printing should be a primary focus initially, though it may depend on other services, such those below, being available. The district will need the ability to cut expense and payroll checks immediately. The best location for check printing may not be at the EOC. It may be at another facility within the district or in a neighboring district.
	2. Terminate district fiber
	3. Terminate AT&T fiber
	4. Install AT&T router
	5. Install AT&T POTS line
	6. District rack(s)
	7. UPS(es)
	8. District Routing Switch including GBICs
	9. Layer 3 switch
	10. Servers for critical district systems as documented in 1-a-I
	11. Telephone system(s) including possible interim POTS lines as necessary
	12. Client access for district tech staff
6. Restore KETS Assets
	1. Move KETS DR rack into place which includes
		1. PDU
		2. UPS
		3. Physical servers for Active Directory
			1. Restore AD from KETS DR site in Azure
		4. Physical servers for ePO & WSUS
	2. Ensure Munis connectivity
	3. Ensure IC connectivity
		1. Facilitate server install with IC if necessary
	4. Ensure CIITS connectivity