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

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
    a. Assesses the situation and declares/confirms a disaster, or crisis
    b. May lead recovery effort, or delegate to others
    c. Provides single point of contact for recovery effort
2. Define a Technical Recovery Lead (HW, SW, systems, facilities, etc.)
    a. Contacting stakeholders to inform and request action
        i. Vendors such as Dell, Tyler Tech., local power, phone, etc.
    b. Getting systems back on line via backups
    c. Coordinate with Business Recovery Lead
    d. Updates DR Plan
3. Define a Business Recovery Lead (Legal, processes, communications, etc.)
    a. Contacting stakeholders
        i. Insurance
        ii. The Media
        iii. Emergency Medical Technicians
    b. Coordinate with Technical Recovery Lead (may be same person)
    c. Updates DR Plan
4. Document All Key Partners
    a. Systems & Service Vendors
        i. Local fiber vendor
        ii. Electrician
        iii. Low voltage wiring vendor
        iv. HVAC
        v. Network vendor
        vi. Telecom vendor
    b. District Leadership
        i. Superintendent
        ii. Board members
        iii. CIO
        iv. Tech staff
        v. Facilities staff
        vi. Emergency Purchases staff
    c. KDE Leadership
        i. KETS Engineer
        ii. KIDS Office
        iii. KETS Service Desk
    d. Other
        i. EMT Services

ii. Insurance
iii. Local Media (newspaper/radio)
iv. Parents/Legal Guardians

5. Define Subordinate and Backup Leads, as necessary, for Individual Process and Systems
6. Establish a communications plan
    a. Define availability and accessibility expectations
    b. Discuss escalation paths
    c. 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

7. 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:
    a. Disaster - Catastrophic loss of hub site and all systems & assets contained therein. Everything, or nearly everything, is gone. No services are available.
    b. Crisis – Partial loss of hub site systems & assets. One or more critical services are down.
    c. Emergency – One or more critical services are experiencing problems. Physical loss of ingress / egress access to hub site.

STEP 3: Define Critical Technology Assets

8. Inventory your systems
    a. Critical District Systems (onsite or cloud)
        i. Food Service
        ii. Library
        iii. File Storage
        iv. Bus/Transportation
        v. Telephone/Voice/Video
        vi. District Website
        vii. Secure Web Gateway, etc.
    b. Critical Network Hardware
        i. Layer 3 Switch/Core routers
        ii. Uninterruptable Power Supplies
        iii. Include a network Topology Diagram with plan for rerouting the district fiber network to support move of the hub site to another physical location.
    c. Critical Business Continuity Hardware
        i. Check printers, scanners, phones, etc.
    d. Software, especially mission critical applications.
        i. 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?

    e. 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?
9. 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.
    a. Include existing disaster recovery or business continuity plans provided by vendor partners for each system (onsite or cloud)
    b. Define the number of days business can be conducted without each of these systems. You may find several redundant systems
    c. Assign each system a realistic estimate of days to restore, and notify business stakeholders of this timeframe, in order to set their expectations.
    d. Inventory System Data Back-ups
        i. What's backed-up?
            1. Everything?
            2. Only Critical information?
            3. Some of the Critical Information?
        ii. Backup storage location
        iii. Steps to restore from backups
10. Inventory Workstations and peripherals
11. Inventory Privileged Accounts and passwords
    a. What is the purpose of each account?
    b. To which system(s) does each account have access?
    c. Are the passwords to each system account accessible and stored securely?
12. 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
    a. Utilities (water, electric, HVAC - who is your point person and when can I expect services?)
    b. Computer providers (how fast can replacements be on the ground?)
        i. Will they be ready to join our domain?
    c. Software/Critical Application companies (how fast…?)

STEP 4: Identify Alternate Site(s)

13. 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?
    a. Does the proposed site already have the following?
        i. Power
        ii. Lighting
        iii. Network

iv. Phones
v. Office Supplies (Pens/Paper/Whiteboard/Markers/Coffee/etc.)
vi. Water/restroom facilities

b. Is it close enough to be accessible by staff, but far enough away to not be impacted by the same disaster?
   i. Different weather systems (e.g. floods, tornados)
   ii. Different electric grid
   iii. Accessible by main roads

c. Identify travel and accommodation arrangements for critical technology and business continuity staff

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

14. 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.
    a. 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

15. 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.
    a. 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.
    b. 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
   a. Partial loss including… (begin with priority items)
   b. 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:
   a. Facility space appropriated

    b. Physical security ensured
    c. Utilities are hooked up and available
    d. Environmental and comfort controls in place and functioning
4. Set communication plan in motion
5. Begin recovery of critical business systems
    a. 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.
    b. Terminate district fiber
    c. Terminate AT&T fiber
    d. Install AT&T router
    e. Install AT&T POTS line
    f. District rack(s)
    g. UPS(es)
    h. District Routing Switch including GBICs
    i. Layer 3 switch
    j. Servers for critical district systems as documented in 1-a-I
    k. Telephone system(s) including possible interim POTS lines as necessary
    l. Client access for district tech staff
6. Restore KETS Assets
    a. Move KETS DR rack into place which includes
        i. PDU
        ii. UPS
        iii. Physical servers for Active Directory
            1. Restore AD from KETS DR site in Azure
        iv. Physical servers for ePO & WSUS
    b. Ensure Munis connectivity
    c. Ensure IC connectivity
        i. Facilitate server install with IC if necessary
    d. Ensure CIITS connectivity