Learning Continuity Planning

IT Crisis Preparedness

Before a disaster strikes, it is incumbent upon school system IT personnel to have emergency operations plans in place to ensure continuity of learning. Natural disasters can be spontaneous events, requiring school system leaders to implement and train team members on procedures so that they can act swiftly. Administrative and school personnel should be able to assess damage quickly, update all stakeholders, bring critical systems back online, and resume operations as quickly as possible.

COVID-19, or the Coronavirus, has prompted school system leaders to reassess their overall disaster preparedness. Unlike natural disasters, which may be confined to a certain geographical location, the novel coronavirus impacted all school systems in the U.S., thrusting IT leaders nationwide into uncharted waters. Learning Continuity preparedness should include emergency operations planning for public health emergencies, including pandemics. Contagious disease outbreaks such as measles, flu, and COVID-19 are just a few of the public health emergencies that can impact technology operations. School Systems must be prepared to assess the impact of the emergency on operations, update stakeholders, maintain critical systems, support the delivery of key services, and support a responsible restoration of operations once the emergency is under control.

In the worst-case scenario, a school system may face simultaneous emergencies, such as an earthquake or tornado coupled with a pandemic outbreak. Regardless of the nature or scope of the disaster, a carefully considered IT continuity plan, as part of a larger emergency operations plan, is critical for school systems to respond to natural disasters and public health emergencies.

School system leaders should provide all personnel with secure operations and learning continuity plans that they can access remotely. These plans should be safeguarded to prevent them from being compromised by agitators seeking out potential vulnerabilities.

General Disaster Preparedness

The Readiness and Emergency Management for Schools Technical Assistance Center (REMS TA) of the U.S. Department of Education provides in-depth emergency operations planning (EOP) resources for schools. IT crisis preparedness is an important component of any EOP. All school systems should develop an emergency operations plan that includes clearly defined roles and responsibilities for emergency response teams, including IT personnel.

Preparation steps for both natural disasters and public health emergencies

- Identify an owner for the plan. The plan owner is responsible for coordinating the maintenance and testing of the plan. The plan owner should be in a leadership role within the school system and have the authority to access resources to participate in testing and maintaining the plan.
- Consider the potential disruption of regular communication methods when developing communication plans and protocols for before, during, and after the disaster.

- Identify a communications plan and strategy and include them in the plan. Define what information will be communicated and by whom to ensure that only accurate information is being given.
- Set up conference bridges in advance and share the information with the appropriate teams, i.e., cabinet, IT, etc.
- Establish baseline criteria to determine when schools are ready to re-open.
- Consider developing board-approved emergency purchase waivers that allow school system personnel to expedite the repair and/or replacement of damaged IT equipment and facilities. Waivers should be reviewed by the school system's legal counsel.
- Consider getting Government Emergency Telecommunication Service cards for board members and school system emergency operations team members.
- Test the plan. A plan may quickly prove to have significant gaps or oversights if it is not tested. Test the plan using scenarios that make sense to the school system. Consider holding annual or bi-annual tabletop tests of the plan.
- Review and update the plan annually, at the very least. An outdated plan may become a liability in an emergency as vital information may be inaccurate or missing.

Cybersecurity Considerations for Learning Continuity Planning

Natural disasters, public health emergencies, and any other kinds of events that can disrupt normal school system operations is an opportunity for hackers to leverage the disruption to access or attack school systems, steal data, and cause further disruption. Cybersecurity precautions should be included in school systems' learning continuity plan as a critical consideration for all emergency response and business continuity processes.

- Confirm cybersecurity measures and capabilities are in place to counter malicious attacks that can threaten operations and data privacy. See CoSN resources available on the Cyber Readiness tab on the CoSN Cybersecurity Page.

Preparation for Natural Disasters

- Establish a comprehensive inventory of equipment, including physical devices, applications, digital tools, systems, etc., necessary to support the ongoing operations of schools.
- Ensure that wireless hotspots are available for emergency response personnel.
- Develop post-disaster assessment resources, such as damage identification and evaluation templates.
- Establish baseline criteria to determine when schools are ready to re-open.
- Have vendor agreements in place with companies outside the immediate geographical area who are not likely to be affected by the same disaster, including IT and facilities vendors.
- Review FEMA regulations on an annual basis. Work with the agency and local government agencies to do annual regulation reviews, as regulations change frequently.
- Document and take pictures of IT facilities and equipment for FEMA and insurance purposes.
- Consider purchasing backup generators for key locations, such as data centers or emergency command locations.
- Back up key systems such as payroll and finance off-site and determine how financial payments will be made after the disaster. Determine how critical IT systems will be restored in the event that onsite infrastructure is destroyed or inaccessible. Well in advance of any emergency, identify critical jobs and cross-train staff to ensure those functions can be supported.
- Ensure that entertainment options are available for people manning the command center during downtime.

Preparation for Public Health Emergencies

- Review county public health processes and identify key contacts at the county public health department.
- Survey staff, parents, and students to determine the home availability of learning devices and Internet access.
- Ensure that devices and Internet connectivity are available for employees needing to work remotely. Consider deploying wireless hotspots or providing financial support for employees unable to afford home Internet access.
- Ensure that devices and Internet connectivity are available for students needing to access educational resources remotely, such as laptops and wireless hotspots.
- Determine how critical and sensitive functions such as payroll, procurement, and payment approvals will occur in a remote work environment.
- Have vendor agreements in place with companies that can continue to provide services remotely, including IT and education technology vendors.
- Develop post-emergency assessment resources, such as impact identification and evaluation templates.
- Consider investing in multi-factor authentication technologies for remote access to critical systems.
- Determine how critical IT systems will be supported in the event that onsite infrastructure is inaccessible and/or key personnel are ill.

Preparing for Natural Disasters with Advance Warning

For natural disasters for which there may be an advance warning, such as hurricanes, school systems should create a checklist of actions to be taken 72, 48, and 24 hours before the storm.

Time to Storm	Action
3 Days	✓ Confirm teams to perform post-storm site visits. ✓ Ensure teams have the necessary equipment, such as masks, boots, and flashlights. ✓ Provide each team with a digital camera to take time and date-stamped photos after the storm since cellphone cameras don't always offer this functionality.
2 Days	✓ Identify the primary point of contact for each facility. ✓ Confirm that key network and hardware vendors have replacement equipment readily available to expedite post-storm replacement if needed. ✓ Sign necessary forms allowing vendors to ship replacement equipment immediately without going through the regular purchase order process. Policies should be flexible enough to allow for the timely replacement of damaged equipment, but require documentation so as to assure the integrity of the purchase process and meet FEMA and insurance requirements. ✓ Track the number of hours being worked by emergency personnel so as to apply for FEMA reimbursement. ✓ Confirm who needs to receive technology status information post-storm and the appropriate format for transmission. ✓ Ensure the command center has multiple copies of school system maps to assist with the deployment of assessment crews.

1 Day	✓ Have employees unplug their computers and raise them off the floor when possible. ✓ Physically protect network equipment when possible. ✓ Shut down low-priority systems. ✓ Allow individuals who will be working on-site during the event to go home and make necessary preparations. ✓ Gather EOP personnel at the command center. Ensure there are adequate personnel support resources, including food, water, and bedding.

During the Natural Disaster

During the disaster, personnel should monitor network power and disaster status from a secure location, triage remediation in affected areas, and utilize the communications plan/strategy identified in the planning stage to determine what information needs to be shared and with whom, and initiate emergency communications.

After the Natural Disaster

- Allow extra travel time to affected sites due to their potential accessibility. Determine the safest routes of travel and availability of fuel.
- Have facilities teams inspect buildings for structural soundness and air quality before allowing employees to enter buildings.
- Deploy technology assessment teams as soon as it is safe to do so.
- Have assessment team leads collect and report information about conditions at each site.
- Ensure damage assessment information is collected in a centralized location.
- Prioritize the repair of critical technology systems such as payroll and finance.
- Determine if cell phone service is widely available in the local area. Communication outages may be short in some areas, but may last weeks in others.
- Communicate regularly with board members.
- Bring in counselors to help students and staff deal with the event and its aftermath.
- Leverage the school system website to communicate repair status, school closures, and other pertinent information. If necessary, redirect the website to a location that can handle higher traffic and is not dependent on local infrastructure.
- Limit press communications to official channels to ensure the accuracy of data made available to the public.
- Establish official channels through which community members can donate funds or otherwise assist with recovery.
- Track the status of equipment replacement and repairs at each campus.
- Check all video surveillance systems and restore any damaged or disabled systems to functioning so monitoring of physical locations can be restored.

Preparing for Public Health Emergencies with Advance Warning

For public health emergencies for which there is an advance warning, such as pandemics, school systems should create a checklist of actions to be taken 1-5 days before the expected impact to school system services.

Time to Impact	Action
3-5 Days	✓ Leverage the communications plan/strategy identified in the continuity plan to develop a specific communications plan for this event. ✓ Identify the single point of contact for the media. Limit press communications to official channels to ensure the accuracy of data made available to the public. ✓ Confirm the primary point of contact for each facility. ✓ Identify which school system processes may be moved to a remote format. ✓ Ensure staff has the necessary equipment to work remotely, such as laptops, tablets, Internet access, and secure remote access to critical systems. ✓ Plan for distribution of equipment to students to support remote learning. ✓ Track the number of hours being worked by personnel on the public health emergency so as to apply for emergency funds if they become available. ✓ Determine how the IT department will intake and leverage donated equipment. ✓ Confirm the technical support contact information of vendors of your critical IT systems and infrastructure. ✓ Check equipment out to students/parents, either on-site or via delivery to specific neighborhoods.
2 Days	✓ Communicate equipment delivery plan to students and parents and schedule equipment checkout. ✓ Identify who may need assistance with obtaining Internet connectivity for remote learning. ✓ Sign necessary forms allowing vendors to ship equipment immediately without going through the regular purchase order process. This may include directly shipping to end users with a pre-loaded and sanctioned school system build already installed on the device. Policies should be flexible enough to allow for the timely purchase of new equipment, but require documentation so as to assure the integrity of the purchase process and account for the purchases once the school system returns to normal functioning. Consider requesting that the School Board provide approval to bypass the regular purchasing process and utilize an emergency purchasing process. ✓ Identify how items purchased will be received if buildings are closed. Consider directing all purchases to a single location. ✓ Confirm who needs to receive technology status information during the crisis and the appropriate format for transmission. ✓ Ensure school system leadership has accurate data on equipment available for student checkout.
1 Day	✓ Limit remote access to critical systems to the fewest number of personnel possible. ✓ Determine what essential services need to be maintained on-site. For example, services and systems to provide grab-and-go student breakfasts and lunches. ✓ Determine who may be allowed to continue working on-site during the emergency and any safety precautions those staff need to take. ✓ Make sure your video surveillance systems are up and running and monitoring unoccupied buildings

During the Public Health Emergency

During a public health emergency, personnel should monitor network and systems access and activity from a secure location. In addition to normal hardware and software issues, these systems will be at risk as hackers attempt to exploit emergencies to gain access and disrupt systems.

Establish processes and procedures to resolve break/fix issues on student and staff equipment. This process may vary depending on the nature of the public health emergency. Set up systems allowing remote technical support to limit physical contact between individuals during a public health crisis.

If remote support efforts are unsuccessful, additional steps to resolve break/fix issues should consider the following:

- Directions for handling and sanitizing equipment being repaired.
- Steps to minimize physical contact during the hand-off of the equipment IT staff and return of the equipment to staff or students.
- Options to replace the equipment in place, such as shipping or delivering replacement equipment, rather than attempting to repair the equipment during a public health emergency.

After the Public Health Emergency

- Have facilities teams prepared to clean and sanitize buildings before allowing employees to return.
- Have assessment team leads collect and report information about the availability and utilization of remote learning.
- Ensure assessment information is collected in a centralized location.
- Communicate regularly with board members.
- Bring in counselors to help students and staff deal with the event and its aftermath.
- Leverage the school system website to communicate status, school closures/openings, and other pertinent information. The website may need to be redirected to a location that can handle higher traffic volumes than usual.
- Limit press communications to official channels to ensure the accuracy of data made available to the public. Channel all press communications through a single point of contact and focus communications on verifiable facts.
- Establish official channels through which community members can donate equipment, funds, or otherwise assist with recovery.
- Track the status of equipment checked out and returned by staff, students, and parents.
- Develop a comprehensive plan for returning to campus. Depending on the type of public health emergency, this may include the following:
    - Identify procedures for screening staff and students and monitoring for possible symptoms should be established
    - Determine if screening procedures require technical systems in place to capture temperatures and screening question responses and store the data securely
    - Connect with local public health officials to identify the role of public health officials and the school system in monitoring for possible recurrence of the emergency
    - Determine if any changes to daily school processes are necessary, such as changes to class size, scheduling, rotation, etc., and identify and adjust the downstream process. For example, if the

school system shifts to an A/B attendance schedule, identify how to maintain accurate attendance, changes to the bell schedule, etc.
    - Implement processes to maintain cleanliness and reduce the risk that a public health emergency recurs. This may include increasing the volume of critical supplies on hand, including personal protective equipment (PPE) such as face masks, gloves, and cleaning supplies.
    - Identify staffing concerns and considerations, including staff coverage, training, and rotation schedules to reduce the chance of recurrence.
    - For situations where immunization is available, identify requirements for the return of staff and students to work, including any immunization documentation requirements.
- Develop crowd control expectations for potentially high traffic and/or high-risk locations such as nursing offices and sick rooms.

Evaluating Lessons Learned - Natural Disasters and Public Health Emergencies

After a natural disaster and/or public health emergency, identify lessons learned and incorporate them into future IT crisis preparation plans. This important activity should be done in two stages:

- After the immediate crisis has passed, evaluate the emergency response from an IT department perspective while problems are fresh in everyone's mind. Other operational units should conduct their own emergency response evaluations to determine areas for improvement.
- Adjust emergency procedures as needed based on the evaluations done by each operational unit. Soon thereafter, conduct a school system wide post-mortem with cabinet and emergency staff. The post-mortem on the event should focus on areas of success and lessons learned. This is an essential component of responding to a disaster or emergency as the lessons learned can help the school system learn from the experiences, document new processes and solutions to problems and develop a stronger plan.