CoSN
Leading Education Innovation

Building your Learning Continuity Plan or Business Continuity Plan

Produced by the Network & Systems Design Advisory

Building your Learning Continuity Plan or Business Continuity Plan

Why Have a Learning Continuity Plan or Business Continuity Plan?

It is important to have an identified scope when developing an LCP or BCP for your school or district IT organization. It is recommended that IT organizations focus on building a technical plan that helps IT prioritize services and identify strategies for continuing to deliver high-priority services to support the district in the event of a disaster that destroys or severely cripples one or more of the district's data centers, networks, and server systems. This plan is not limited to on-prem systems; cloud services and applications are within the scope of this plan.

While the district's LCP or BCP should encompass the entire district's operations, this document focuses on the information technology components that support the district's overall plan.

Primary objectives of the IT plan should include:

- Identify and prioritize mission-critical systems for recovery and restoration
- Identify key personnel, roles, and responsibilities to support recovery efforts
- Document where to find equipment, procedures, and other items necessary for recovery.

Generally speaking, the plan should include the following components:

Procedures for Activating the Plan

Documenting who can activate the continuity plan and how activation occurs is important. A threshold for activation, such as how long the systems should be down before launching the LCP/BCP, should also be included in the documentation.

The activation plan should include directions for establishing a coordination center or room to operate the recovery.

Safety Considerations: Health, Life and Safety Comes First

Hazards and dangers can abound in almost any disaster situation. While surviving the disaster itself can be a harrowing experience, further injury or death following the disaster stemming from carelessness or negligence is senseless.

Include in the plan the expectation that all personnel must exercise extreme caution to avoid physical injury or death while working in and around the disaster site itself. No one is to perform any hazardous tasks without first taking appropriate safety measures. Work with both your district and local authorities as to when and where you can access the site.

Personnel

- Document key personnel and how to contact them. Include two methods of contact in case one method is offline. Make sure to include a backup contact. The person you need may not be available in an emergency.
- Document roles and responsibilities for a disaster scenario in a responsibility assignment matrix or RACI chart (https://en.wikipedia.org/wiki/Responsibility_assignment_matrix).
- Identify where people will meet if there is a disaster and identify a secondary location.

Backups

- Avoid storing your backups with your primary system. Backups should be stored in a separate geographic location.
- Regularly test your backups
- Have a plan to restore both the system and the data
- Review your backup plan and configurations annually
- Review your cloud contracts to determine what your providers do for backup and recovery

Recovery Location

Plan access to a recovery facility through a hot site, cold site, or cloud computing.

- **Recovery Facility:** If a central facility operated by the Technology Department is destroyed in a disaster, repair or rebuilding may take an extended period.

In the interim, it will be necessary to restore the computer and network services at an alternate site.

- **Hot Site:** This is probably the most expensive option for preparing for a disaster and is typically most appropriate for large organizations. A separate computer facility, possibly even located in a different city, can be used, complete with computers and other facilities ready to cut in on a moment's notice if the primary facility goes offline. The two facilities must be joined by high-speed communications lines so that users at the primary campus can continue to access the computers from their offices and classrooms. This assumes network connectivity is available.
- **Cold Site:** A cold recovery site is an area physically separate from the primary site where space has been identified as the temporary home for the computer and network systems while the primary site is being repaired. There are varying degrees of "coldness," ranging from an unfinished basement to space where the necessary raised flooring, electrical hookups, and cooling capacity have already been installed, just waiting for the technology to arrive.
- **Cloud Site:** A cloud recovery means bringing your systems up in a cloud data center providing Infrastructure as a Service so you can restore your systems to an outside environment. This option is dependent upon network connectivity. However, it can be a very fast and cost-effective solution as these environments can be spun up as needed with a cloud hosting provider. This is an expensive approach to run for long-term use, depending on the amount of data transiting in and out of your systems, but very viable for recovery efforts.

Process for Assessing Damage to Systems

Document a process for assessing damage and recovery requirements. This can include the following steps:

- Determine which hardware, software, and supplies will be needed to start restoring a particular system. This should include documentation of system dependencies. For example, network capabilities such as DHCP, DNS, and authentication need to be restored ahead of services that depend on these basic network capabilities.
- Process for ordering replacement components

- Emergency procurement procedures.

Prioritized List of Systems to Recover

- The plan should include a prioritized list of systems to recover based on completing a Business Impact Analysis.
- See Identifying and Prioritizing Critical System Risks
- See Disaster Recovery Plan Template

Disaster Recovery Plans for High-Priority Systems

- Document recovery steps and plans for each high-priority system
- **Test** the recovery documentation to ensure systems can be restored based on the directions. Identify any dependencies for restoration, including network access, login capability, access to on-prem or cloud resources, etc.
- Document the current backup system and its location. Backups should not be stored in the same physical location as the systems being backed up.
- Backups should be tested regularly to ensure systems and data can be restored.
- Document processes to access backups.

Communications Plan

Identify who will coordinate communications with district leadership and with the public if necessary. Leverage a communications planning matrix to make this process more streamlined.

Criteria for Disaster Conclusion

Determine what criteria must be met for declaring a disaster at an end.

Testing the Plan

Identify strategies and schedules for testing the plan. This should include tests of system and data restoration from backup and scenario-based tabletop exercises designed to practice the LCP/BCP processes and procedures.

Recommended Appendixes to Include as Separate Documents:

System & Application Disaster Recovery Plan(s)

Appendix A: Contracts and Agreements

Appendix B: Internal Contacts

Appendix C: External Contacts

Appendix D: Maps, Floor Plans and Diagrams

Appendix E: Sample Forms/Documents

Appendix F: Processes and Procedures

About CoSN: CoSN is the premier professional association for K-12 EdTech leaders, their teams, and other school district leaders. CoSN provides thought leadership resources, community, best practices, and advocacy tools to help leaders succeed in the digital transformation. CoSN represents over 13 million students and continues to grow as a powerful and influential voice in K-12 education. CoSN also provides opportunities for companies that support the K-12 EdTech community to participate as corporate members.

CoSN is vendor neutral and does not endorse products or services. Any mention of a specific solution is for contextual purposes.