

Continuity of Operations Planning Guide

Technology Considerations

Contents

Credits	1
Introduction	2
Purpose	2
Terminology	2
Scope	2
How to use this guide	3
Developing a COOP	4
Objective	4
Forming a Team	4
Identifying Critical Functions	6
Timing of the Event	6
Alternate Service Location Considerations	7
Safety & Security	7
Interdependencies	8
Additional Considerations	8
Technology Systems Inventory	9
Communication Systems	9
Facilities	12
Food Services	15
Network Services	16
Transportation	19
Student Services	21
Finance, HR and Payroll Systems	24
Appendices	25
Critical Functions Checklist	25
Continuity of Operations Planning Worksheet	27
Glossary	28

Credits

This document was developed by MAISA (Michigan Association of Intermediate Superintendents) through its leadership network METL (Michigan Education Technology Leaders). METL consists primarily of ISD/ESA/RESA senior technology leaders from across the state of Michigan. Contributions were also made by [MiCloud](#), [MiSecure](#) and [MiSEN](#), providing statewide leadership in cloud infrastructure, cybersecurity and networking, respectively.

Introduction

Purpose

Districts depend on a wide range of systems to support daily operations, spanning teaching and learning, communication, and administration. While technology brings efficiency and coordination, its failure - whether isolated or widespread - can seriously disrupt a district's ability to function. Continuity planning helps address this risk by identifying the role of each system, assessing how failures could affect other areas, and considering alternative tools or processes to minimize operational disruption. Because many systems are interconnected, the failure of one can trigger cascading effects across multiple departments. This highlights the need for thoughtful planning and cross-departmental collaboration.

Terminology

Every effort has been made to reduce the number of technical terms throughout this document. While it will occasionally be necessary to use some technical terms, it is expected that IT staff will be participating in this planning process and can address these; however, a full glossary is available at the end of this document. In addition, the terms below have very specific definitions as used within this document.

Term	Definition	Example
Server	A physical or virtual computing device that provides one or more services	A Windows server providing file and print services for the district
Service	An application(s) that performs a particular task. The application could be running on a server in the district's data center or provided by a 3rd party in the cloud.	A Student Information System (SIS) runs on a server to provide attendance and grades
System	Multiple components (servers, services and devices) that perform a specific task. The term "system" will often be used generically.	A video security system which may include a server, specialized software running on the server and video surveillance cameras

Scope

A comprehensive Continuity of Operations Plan (COOP) is a framework developed by a district to ensure that essential functions can continue during and after a wide range of emergencies, including natural disasters, technological failures, international incidents, or other catastrophic events. The primary goal of a COOP is to ensure that a district can ***continue to perform its essential functions*** during and after a wide range of emergencies or disruptions.

Traditionally, COOPs focus on large-scale disasters (such as the loss of a building) and don't address the underlying technologies providing specific, key services for a district. As district reliance on technology increases, these individual systems can become the actual cause of the disruption, and

their importance needs to be individually considered. Furthermore, since technology is constantly changing, a district's COOP must be regularly reviewed for updates.

A COOP is activated when an organization faces a disruption that prevents it from performing its essential functions. These trigger events can be broadly categorized as:

- **Technological Failures:** Network and/or Internet outages, cyberattacks (ransomware, data breaches), critical system failures, or telecommunications disruptions
- **Natural Disasters:** Hurricanes, tornadoes, floods, earthquakes, wildfires, blizzards, or pandemics
- **Human-Caused Incidents:** Active threats, terrorism, civil unrest, or widespread criminal activity
- **Infrastructure Failures:** Utility failures (power, water, gas), transportation disruptions affecting staff or supplies, or significant facility damage.
- **Personnel Disruptions:** Sudden loss of key personnel due to illness, injury, or other emergencies that impact leadership or critical staff availability

This COOP planning guide has been developed through an information technology lens. Districts are encouraged to consider non-technology-related disruptions, especially in relationship to other existing plans such as a district Emergency Operations Plan, Disaster Recovery Plans, and Cybersecurity Incident Response Plans.

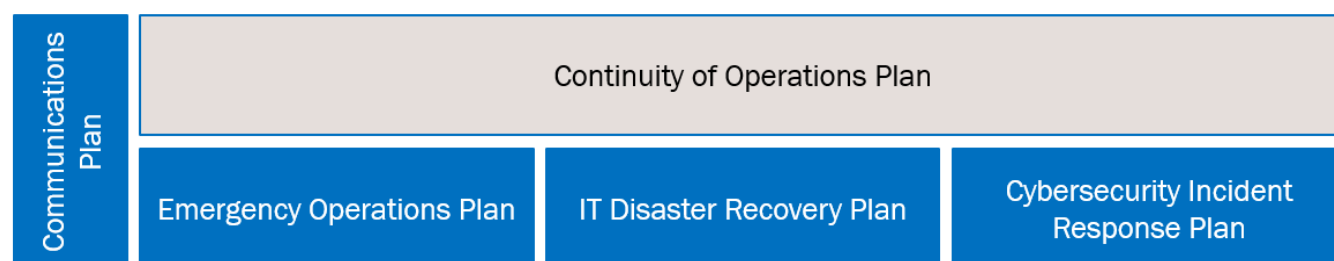


Figure 1. Essential District Contingency Plans

How to use this guide

This guide provides districts with a structured approach to analyzing potential challenges that may arise from the unexpected loss of one or more technology systems. While not a COOP template, it does outline key considerations for technology services that support the development of a comprehensive plan.

Though obvious, the best time to discuss the district's approach to continuity of operations is before a disruption occurs. Proactive planning helps minimize interruptions to student learning and other essential district functions. This guide outlines common technology systems and their potential roles in supporting operations. However, it is not an exhaustive list - districts may use additional tools not mentioned here, and some systems may not apply to all settings. Leaders are encouraged to collaborate with stakeholders to tailor this resource to their district's unique environment.

Developing a COOP

Objective

As noted earlier, this document is not intended to serve as a COOP *template*; although it can be a useful starting point. Districts should determine the format that best suits their needs. A final plan might take the form of a prioritized list of systems to restore or a comprehensive document that includes all services, servers, systems, alternatives, dependencies, restoration procedures, vendor contacts, and more. It could be a standalone plan or integrated into an existing Emergency Operations or Disaster Recovery plan. Regardless of its format, this document is designed to guide thoughtful discussion around the key considerations for developing an effective COOP.

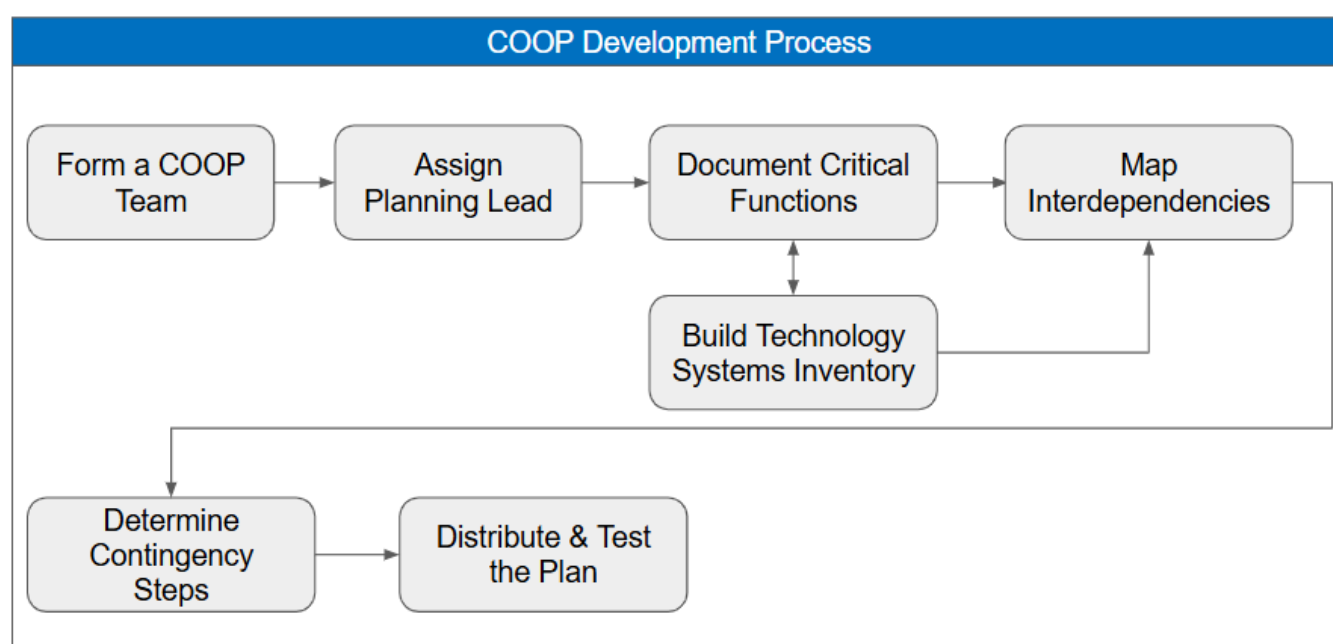


Figure 2. Example COOP Development Process

Forming a Team

While this COOP guide has a technology focus, the actual impact and responsibilities lie within all departments. Therefore, when developing a COOP, it is critical that each department is represented by a person(s) that fully understands the impact of their systems on overall school operations. The size of this team will likely be dictated by the size of the district, but in general, representation could include:

Department	Example Roles
Functional area: Instruction and Student Support	
Curriculum & Instruction	Curriculum Director

Department	Example Roles
Special Education	Special Education Director, Program Supervisor
Student Services	Social Worker, Attendance Coordinator
Career & Technical Education	Director of CTE, Work-based Learning Coordinator
English Language Learners	Director/Coordinator of ELL, ELL Coaches
Functional area: Operational and Administrative	
Human Resources	HR Director, HR Generalist
Finance & Business Services	Business Manager, Payroll Specialist
Facilities and Maintenance	Facilities Director, Maintenance Supervisors
Transportation	Transportation Director
Food Services	Food Service Director/Supervisor
Technology Services	CTO, IT Director, Network Administrator
Communications	Communications Director
Safety & Security	Director of School Safety, Security Operations Manager
Functional area: District Leadership	
Superintendent's office	Superintendent, Assistant Superintendent
Building Leadership	Principals, Assistant Principals

Figure 3. Example Team roles

As part of the COOP process, team members must identify the technology systems their department depends on and determine potential temporary measures if those systems become unavailable. Departments may not fully understand the consequences that the loss of one or more systems may cause. For instance, if a student information system (SIS) is unavailable, teachers would not be able to submit attendance and enter grades, but also, parents may not be able to review their child's schedules. To capture all of the impacts each system may cause, districts should consult with other stakeholders such as teachers, parents, law enforcement, mechanics, vendors, and students to make these identifications.

COOP Planning Lead

One member of the COOP team should be designated as the Planning Lead. The Planning Lead role is critical in helping the district coordinate the complexities of creating a comprehensive COOP.

- Coordinate a kickoff meeting with the COOP team (from roles identified above)
- Share the [Critical Functions Checklist](#) from the appendix. This list will help team members to identify all potential systems from their department
- Work with the team to decide on the format of the final product

- Schedule regular future meetings to review and update the plan

Identifying Critical Functions

Once the COOP Team is established, the next step is to identify the organization's critical functions. A critical function is defined as one that, if not performed, would significantly impair the district's ability to achieve its mission, meet its legal obligations, or ensure staff and student safety. Keeping in mind that the scope and scale of critical functions will vary by organization, the following examples demonstrate how you can document your district's critical functions and their potential impact if unavailable.

Critical Function	Department	Supporting Technology	Contingency Steps
Payroll	Business Services	ERP (Enterprise Resource Planning) System, Network, Internet	Manually process payroll
Door Access System	Safety and Security	Door system server, Network	Manual Locking of Doors, Security Guards
Mass Communication	Communications	Notification System, Network, Internet	Fallback to email Use public website

Figure 4. Example Critical Functions

Use the [Critical Functions Checklist](#) in the appendix to identify the functions that **must** be operational in order to safely conduct school for staff and students. Within each function there are multiple subsystems that may or may not be required from a legal, code, policy, or safety perspective. Check off those functions and subfunctions which are required to keep schools open.

A critical function may be reliant on one or more technology systems. The [Technology Systems Inventory](#) section below provides explanations and questions to help determine which systems are required to operate, how the loss of each system might impact service delivery, and what steps might be taken to ensure continuity of operations. Reviewing each of these sections with corresponding department personnel will ensure that inter-dependencies are captured.

Once you complete the critical functions checklist, you may want to use the [Continuity of Operations Planning Worksheet](#) at the end of this document to document your systems, dependencies, and steps for operational continuity. Again, refer to the [Technology Systems Inventory](#) section to guide you through the worksheet.

Timing of the Event

Timing of events can impact the district's response. While reviewing each essential operation or service area, consider how a response may differ if the outage occurs:

- Prior to School
- During School
- After School Hours

- During weekends, breaks or holidays
- During payroll
- During statewide testing
- During parent-teacher conferences
- The day before a state reporting deadline
- During a school board meeting

The decision to alter the school day is a time-sensitive process that balances safety with the need for clear and timely communication. Consider what the cutoff time may be for the district to decide if school will be operational for that day by using a work backwards from time constraints approach when developing the COOP. Surprises may develop as additional stakeholders review the assumptions around timing and impact.

Alternate Service Location Considerations

In many situations, your organization may lose physical access to one or more data centers. If this happens, you must determine where and how to establish temporary services. Your alternate location could be a nearby school district, a university, a partner organization, or the cloud ([MiCloud](#) is available to help you set up cloud infrastructure). Because various disasters can impact each choice, you should develop multiple backup options.

When planning, make sure to evaluate:

- Whether you have the necessary infrastructure to run a basic, minimally functioning alternate site.
- How your team will physically or digitally access the location.
- How you will restore your critical systems to that new site.

Test these options as much as possible. While you may not be able to fully simulate a total data center failover, you can often test restoring and running one or two critical systems at your backup site.

A comprehensive plan for these scenarios is called an **IT Disaster Recovery Plan**, which is a vital part of your overall readiness. To see how these different technical response plans fit into this broader continuity of operations guide, see the diagram in **Figure 1 on page 3**.

Safety & Security

Your primary systems were designed with strong security in mind, and your backup systems must meet that same standard. During a disruption, staff may need to use unfamiliar tools or processes to keep operations running. These alternatives are often adopted quickly and may lack the security controls of your regular systems. As a result, sensitive information might be transmitted without proper encryption, stored insecurely, or left behind when it's no longer needed. Some additional security considerations include:

- Access Control & Authentication: Ensure backup systems require strong authentication and MFA whenever possible. Use “least privileged access” policies, limiting access to only essential personnel, just as with primary systems.

- Data Integrity and Validation: Confirm that backup systems haven't been tampered with or corrupted before use - especially if the outage event is related to cybersecurity.
- Logging and Monitoring: Make sure backup environments generate logs and are monitored for unusual activity. Logs should be retained and reviewed as part of post-incident analysis.
- Training and User Awareness: Make sure staff are trained on secure use of alternative systems and know to avoid risky shortcuts (e.g., texting sensitive info).
- Data Retention and Cleanup: Have a plan for securely deleting or archiving data created or shared through backup systems after normal operations resume.

Interdependencies

- **Mapping Connections**: Visualize how systems interact and rely on each other. This helps identify potential vulnerabilities and dependencies. You could use a whiteboard and map out dependencies between systems.
 - Identify single points of failure
- **Critical Path Analysis**: Determine the critical path for essential processes and identify the systems involved.
 - Map how data moves between systems
 - Identify which shared resources are used by multiple systems (ie server-database)
 - Evaluate how systems rely on external services or vendors
- **Examples Of Interdependencies**
 - Student Information System (SIS): Relies on the network infrastructure, servers, databases, and operating systems.
 - Learning Management Systems (LMS): Depends on the network infrastructure, servers, and authentication system
 - Email: Relies on the network infrastructure, email servers, authentication servers, and directory services

Additional Considerations

While beyond the scope of this document, a comprehensive COOP will consider the following areas:

- **Staff Roles and Responsibilities**: Clearly define the roles and responsibilities of staff members in supporting critical systems.
- **Testing and Exercises**: Conduct regular tests and exercises to validate the COOP plan and ensure staff preparedness.
- **Vendor Management**: Establish relationships with key vendors and outline contingency plans for vendor disruptions.

Technology Systems Inventory

District technology systems can be logically divided into 7 different categories:

- Communication
- Facilities
- Food
- Network
- Transportation
- Student services
- Finance/HR/Payroll

Specific **examples** and **questions** are provided for each category. In some cases, **possible consequences** are also included. Not all districts will have the same systems. Within each category, the district first needs to identify the existing resources. The [Critical Functions Checklist](#) in the appendix provides a detailed checklist to help identify existing systems.

Once the inventory is established, the district should consider:

- In the event of a complete or partial loss of the system, what would be the impact on district operations?
- How long can the district function without this system?
- What is the priority of this system compared to other systems?
- What other systems might be impacted by the failure of this system?

Communication Systems

Being able to reach parents, students, and staff - especially during a crisis - is critical. While other methods may be available, they may not function in the same way or at the expected speed as those the school normally relies on. These systems manage communication between school buildings, staff, parents, emergency responders, and external stakeholders.

Examples

Email, VoIP phone systems, cellular communication backups, fax services, public announcement systems (PA), digital signage, mass notification platforms, website, social media, short messaging systems (SMS), mobile apps, radio, emergency communications systems (e.g., 2-way radios or satellite-based systems)

General questions to consider during or before a disruption

- What systems do you rely on to communicate internally among staff? How do you communicate with all staff in an emergency?
- What is your plan for communicating with parents, students, and other stakeholders?
- What alternative communication methods are available (e.g., email, phone, radio, social media, website)?

- Who is responsible for managing communications during an incident? Who is secondary if the primary person responsible is unavailable?
- What are the specific roles and duties of individuals in the communication process?
- What information needs to be communicated during different types of incidents?
 - Are there predefined templates or protocols for different types of messages?
- If your organization's primary communication system is down, how will contact information for key personnel, staff, and emergency responders be accessed?
 - Where and how regularly is this maintained?
 - How will this be accessed if the location is digital?
- What secure communication platform will you use to communicate sensitive information when primary systems are down?
- Are parents and other stakeholders aware of alternative communication methods (i.e., if phones are down, we will use...)?
- Does the district have backup circuits for communication for both phones and Internet?
- Consider how long you can function without this communication service?
- What is the priority of this service compared to other services?
- What other systems might be impacted by the failure of this system?

Possible consequences

- Delayed emergency response and inability to contact 911 or first responders
- Failure to alert staff, students, or parents during crises like lockdowns or evacuations
- Spread of misinformation due to lack of official updates
- Disruption to daily operations, including attendance, transportation, and class coordination.
- Loss of trust from families, staff, and the community.
- Increased safety risks for students, especially those with medical or behavioral needs.
- Legal and compliance exposure due to failure to notify or act in time.

Most common critical systems | Special considerations | Specific systems

Digital Signage/Emergency Notification/Public Announcement Systems

Districts typically have systems that manage local, mass communications. Such systems may control digital displays both inside and outside of the district buildings, emergency alert systems, or public announcement (PA) systems for classrooms. These systems allow for coordinated communications, informing students, staff, and visitors about school activities, updates, last-minute changes of plans, as well as communicating emergency notifications. Ancillary systems may also exist, such as digital media players or screen generators.

Specific questions to consider:

- Where are your signs located?
- How are they connected? (i.e., Ethernet, wireless, analog)
- What messages will be on the signs if they lose communication with the main controller?
- How will district-wide alerts be communicated without these systems?

Possible consequences:

- Students/Staff/Community may not be alerted to important information

- Special needs students may be impacted more than others
- Misinformation or lack of current information
- Reduced situational awareness

Facilities

These systems provide management over the physical premises. They control the heating & cooling of the building, monitoring the safety of those in the building and physical access to the building. They may also control lighting, logging in and out of visitors, signage to make announcements - both internally and externally - and provide visitor information.

Examples

Door/access control systems, Video surveillance systems, HVAC controls, Lighting controls

General questions to consider during or before a disruption

- Who is responsible for the management of the system as a whole?
- Are different people responsible for individual components of the system? For example, IT may be responsible for access to a video surveillance system, the vendor may be responsible for the operation of the cameras, while facilities may be responsible for the installation and maintenance of the actual cameras
- What is the impact on student safety, especially for our more at-risk student populations?

Possible consequences

- You may need to develop human-based backup systems to provide support during emergencies

Most common critical systems | Special considerations | Specific systems

Door/Access Control System

This system manages the locking and unlocking of doors throughout your buildings. It generally operates on a schedule and can alert appropriate staff if doors are left ajar. These systems are often managed by a third party, creating additional challenges.

Questions to consider:

- What is the default position of the locks if the *system* suddenly loses power?
- What is the default position of the locks if the *individual* doors lose power?
- Are there any doors that default to “open”?
- Is there a manual override to gain entry?
- If this system is down, how can you admit visitors, staff, and students?
- Do you need signs alerting visitors? What should they say? On which doors?
- Is there a map of doors being managed by the system?
- Is the system backed up regularly?
- Does this system require any special hardware or software?
- Who is responsible for updating the system?

Possible consequences:

- You may need to provide staff to monitor key entry points and greet visitors.
- You may need to provide alternative ways to lock or unlock entrance doors.

- Some sensitive internal doors may also require attention.
- Are you prepared to hold school without properly locking doors?

Video Surveillance System

This system records the video from cameras located inside and outside of the school buildings. This may be one or more systems. The system may be located in the cloud rather than on-premises. The cameras provide the district a measure of security, recording student, staff, and visitor activity.

Questions to consider:

- How does the unavailability of camera and recording software impact security monitoring, surveillance, and safety protocols within the school premises?
- Are you prepared to hold school without access to cameras & recording?
- What support mechanisms are available to assist security personnel in managing the impact of the software unavailability on their surveillance responsibilities?
- Are there manual security procedures or backup surveillance systems available to compensate for the unavailability of camera and recording software?
- How do you access the video surveillance system? Does law enforcement require access to it?

Possible consequences:

- Some cameras may be located in high-security areas and human monitoring may be required to ensure the safety of students.
- In some cases, student safety may be compromised due to the inability to monitor cameras.
- Missed capture of event needed for a response related to school, staff, or student safety.

HVAC System

Maintaining the heating and cooling of buildings provides a comfortable learning environment but also protects the infrastructure and assets.

Questions to consider:

- How does the unavailability of the HVAC system impact indoor air quality, temperature regulation, and overall comfort within the school premises?
- How will the unavailability of the HVAC system affect the health and safety of students, staff, and visitors, especially in extreme weather conditions?
- What measures are in place to mitigate health risks associated with poor indoor air quality or inadequate temperature control during the disruption?
- What support mechanisms are available to assist maintenance personnel in managing the impact of the HVAC system unavailability on their responsibilities?
- Who is responsible for the system? Do you have the contact information for your software provider easily accessible?
- Would a cyber attacker be able to force systems offline or otherwise create settings that could cause physical damage to district infrastructure?

Possible consequences:

- Establish guidelines for temperature and air quality levels that allow for safe instruction and work.

- Possible physical damage due to frozen pipes or developing mold.
- Ensure that there are established emergency limits that maintain non-freezing temperatures if control systems fail.

Lighting Controls

Automated lighting controls - both inside and outside of buildings - can reduce electric expenses as well as provide safety and security.

Questions to consider:

- Are you prepared to hold school when the lighting control system is unavailable?
- What specific functionalities of the lighting system are affected by the cyber incident?
- How does the unavailability of the lighting system impact building occupants and safety?
- What support mechanisms are available to assist maintenance personnel in managing the impact of the lighting system unavailability on their responsibilities?
- Who is responsible for the system? Do you have the contact information for your software provider easily accessible?

Possible consequences:

- Facility safety concerns with low or no light conditions both interior and exterior
- Motion sensors may not function properly during critical times
- Leaving facility lighting illuminated beyond scheduled hours incurs additional utility expenses

Food Services

These systems, usually self-contained, manage and account for the point of sale, track staff assignments and meal deliveries, and possibly orders of food and supplies.

Examples

Food services management systems, point-of-sale devices, ordering systems

General questions to consider during or before a disruption

- How does the unavailability of the food service software impact meal planning, preparation, distribution, and tracking?
- How will the unavailability of the food service software affect the ability to ensure compliance with safety and nutrition regulations?
- How will meal inventory be managed, and how will food supplies be monitored and replenished without food service software?
- Who is responsible for the system? Is the contact information for your software provider easily accessible?
- Is Food Service handled in-house (self-operated) or is it contracted through a 3rd party?
- Are there any implications for federal funding?

Possible consequences

- Establish systems to manually manage food payment and distribution.
- Work with vendors to understand the impact of the loss of internet access on the functionality of food service systems.
- Review synchronization processes when systems are restored.
- Consider how a compromised ordering system might be abused to redirect orders or financial payments.

Most common critical systems | Special considerations | Specific systems

None currently identified

Network Services

Network services provide the foundation for a district's technology operations. They are also the most complex and vulnerable and therefore most prone to a disruption. These services also have the most impact on other systems. For instance, if a district loses Internet access, many of the other systems in this guide will be unavailable, and most will be impacted to some extent.

Examples

DNS (Domain Name System), DHCP (Dynamic Host Configuration Protocol), firewalls, authentication, internet access, local network access, web content filters, authentication services, general file server, network access to other districts, and access to cloud services such as Azure or Google are all essential components of a modern network infrastructure

General questions to consider during or before a disruption

- To what extent is the district reliant upon Internet access for overall operations
- Are users able to authenticate to the network? If not, are they able to use their devices?
- If students aren't able to access the local network, can they participate in learning?
- If staff aren't able to access the local network, are they able to provide instruction?
- Are students able to access web-based content if there is no content filter available?
- If your organization's link to its ISD or other partner organization, does this impact your organization's ability to function?

Most common critical systems | Special considerations | Specific systems

Internet Access

Access to the Internet was once an enhancement to the school environment, but for many districts, it has become operationally critical.

Questions to consider:

- Which services will be completely unavailable if the Internet goes down?
- Which services may still be functional, but impacted in some way? How are they impacted?
- Is there an alternative or backup Internet service? Is that service an adequate, temporary replacement? What works differently and how?
- How long can the district function without internet access? Or on a backup service?

Possible consequences:

- Loss of access to remote systems which may be critical to district operations
- Inability for remote access to critical systems such as power, HVAC, or security systems

Local network access

Access to the district network is separate from Internet access. Staff and even students may very well have an alternative to a district's Internet service using personal devices such as phones. But the loss of services that are typically available on the district's network -even without Internet access - may

cause other operational problems. Districts rely on local switches and wireless networking services to provide access to the local network.

Questions to consider:

- What services would be impacted by the loss of a switch, inter-building access and/or wireless networking?
- What impact will the loss of any locally provided services such as printing or faxing have on operations?

Possible consequences:

- The loss of local network access likely means the loss of access to all network services
- Students and staff will not have access to the Internet unless they can use their own personal devices

Operational Systems (DNS, DHCP, Network monitoring, SEIM, Firewall, Remote access)

In addition to the actual connectivity provided by Internet and local network access, several services exist to support that connectivity. Such systems can have an impact on just one population, area, or operation. Some systems protect

Questions to consider:

- What systems are dependent on DHCP for addressing?
- Have backup DNS servers been identified and tested?
- Is replacement firewall hardware quickly available?
- How can staff remotely access the network?

Possible consequences:

- The loss of one or more operational systems can have very unpredictable consequences, possibly manifesting as a loss of other services.
- Inconsistent access to services; some systems may appear to be operational to some users and not available to others.

Access to cloud-hosted services (e.g. Google, AWS, Azure)

These systems manage accounts, groups, applications, and devices for the organization but are located in the cloud. That is, they do not run on local servers, but rather on a large group of servers to improve reliability. While they are less likely to go down, their service can still be disrupted for many reasons, including Internet connectivity, service provider failure, or misconfiguration.

Questions to consider:

- Do mission-critical services depend on access to cloud services like Google or Microsoft?
- Consider whether the service itself is down or if local or regional access to the service is the issue
- Are there on-site or alternative methods to access the service, such as via personal devices?
- Are you prepared to hold school if users are unable to log in or applications such as email and if network drives are unavailable?

Possible consequences:

- Fallback to manual recording and processing of information until systems are back online
- Increased risk of human error or incomplete records
- Delays in receiving and responding to electronic communications

Transportation

Transportation systems manage bus routes and communication between drivers and the bus garage. Additional systems may provide information on specific needs for special needs students.

Examples

Bus routing, dispatch communications, resources for bus drivers for students with particular needs

General questions to consider during or before a disruption

- Are you prepared to hold school when the transportation system is not available?
- What specific functionalities of the transportation software would be affected by the cyber incident?
- How might the unavailability of the transportation software affect the ability to track and monitor the location of buses and ensure timely arrivals and departures?
- How will transportation logistics be managed manually or through alternative means during the disruption?
- What is the primary method for parents to contact the transportation department, and how would that change if the system (e.g., phone system linked to software, online portals) were unavailable?
- Who is responsible for the system? Do you have the contact information for your software provider easily accessible?
- How would you communicate with emergency services or other external partners regarding bus locations or incidents if your primary communication tools tied to the system were down?
- What other district systems (e.g., student information system, HR/payroll, parent communication platforms) are directly linked to or feed data into the transportation management system? How would their functionality be impacted by an outage?

Possible consequences

- Transportation delays
- Unwanted media coverage
- Significant stakeholder dissatisfaction
- Heightened community concerns

Most common critical systems | Special considerations | Specific systems

Student Transportation Management / Bus Routing and Dispatch

Student transportation management encompasses the systems and processes used to safely and efficiently transport students to and from school and school-related activities. This involves various aspects, including route planning, vehicle maintenance, student tracking, parent communication, and regulatory compliance.

Questions to Consider:

- Did you print hard copies of the individual bus routes (route books) before the start of school?

- How often are you updating route books with student changes?
- When is your critical timeframe for building bus routes?
- What would you do if the system is unavailable during the first two weeks of school?
- Who are the key personnel with the knowledge and authority to manage transportation operations manually if the system is unavailable, and are their roles and responsibilities clearly defined?

Possible Consequences:

- Delays in student transportation
- Issues with substitute drivers
- Manual data collection (attendance)
- Student safety due to missed pickup

Bus Location Tracking (GPS)

GPS tracking solutions are available for K12 school buses, typically focusing on features critical for student transportation: safety, efficiency, and communication. GPS tracking software may integrate with, or be a component of, school bus management software.

Questions to Consider:

- How and how often is your GPS fleet tracking data backed up? Where are these backups stored (on-site, off-site, cloud)?
- If the primary GPS fleet management system becomes unavailable, how quickly could you access the most recent location data for all buses, and in what format?
- If real-time GPS tracking is unavailable, what is your immediate plan to monitor bus locations and ensure routes are completed as scheduled?
- What is your process for dispatching substitute drivers or re-routing buses in real-time if the GPS is down?
- Do drivers have immediate access to printed maps or alternative navigation aids that could be used if their primary GPS-enabled devices or in-bus systems fail?

Possible Consequences:

- Delayed emergency response
- Lost or missing buses
- Lack of accountability

A GPS fleet tracking outage can quickly escalate from an inconvenience to a serious operational, financial, and safety crisis for a K-12 school district, underscoring the need for robust COOP planning.

Student Services

These systems provide staff with information about students - their attendance, performance, contact information, and possibly critical health, medical, or special needs. Some districts may also have systems that provide students with access to online learning or additional resources for their classwork. Teachers may rely on systems that monitor and can control student use of technology during instruction.

Examples

Student information systems, attendance tracking, testing services, learning management, and classroom monitoring systems

General questions to consider during or before a disruption

- What information is regularly accessed from these systems?
- Can functions of the software, such as attendance, be conducted in another manner?
- How long can instruction continue without this system being available?
- Are there backup plans for each system?

Possible consequences

- Classroom management might be impacted
- Required reporting may need to be done using another method
- Necessary student information may not be available (e.g. medical, parent contact, guardianship)

Most common critical systems | Special considerations | Specific systems

Student Information System (SIS)

Description/Purpose: This system manages the data around student grades and participation, and is often a hub for communication between the school and home. It also may provide additional information about students such as medical or special needs.

Questions to consider:

- Do you use your SIS for parent/guardian communication?
 - Is your SIS on premises or remotely hosted?
 - How do you access your SIS?
- What alternative communication channels will be used to relay important information?
- How will essential academic and administrative tasks be carried out if the SIS is inaccessible?
 - Attendance, grading, state reporting, discipline tracking
- Are there offline methods to access the medical needs of students?
- Do you rely on this system for any information on special needs students?
- Is the system backed up regularly?
- Does this system require any special hardware or software?
- Who is responsible for updating the system?

Possible consequences:

- Printing class lists for attendance, pulling reports from backups, providing critical medical services to specific students, attending to the special needs of specific students
- Inability to access critical student data, including medical alerts, emergency contacts, IEP/504 plans, and custody information-potentially compromising student safety and compliance.
- Disruption of essential operations like attendance tracking, grading, scheduling, state reporting, and discipline management-leading to administrative delays and potential audit issues
- Breakdown in parent/guardian communication, especially if the SIS is the primary platform for mass messaging or notifications.
- Manual workarounds increase staff workload and risk of errors, such as inaccurate attendance or grade entry once systems are restored.
- Compliance risks and potential data exposure, especially in breach scenarios, which could trigger legal obligations, state/federal reporting, and loss of trust with families.

Learning Management Systems (LMS)

Some districts may have systems that provide online resources in support of in-person learning and/or testing. These systems may also provide access and support for fully online classes.

Questions to consider:

- Will students who utilize these systems for online learning be able to access their classes in another way?
- If staff use the system to support their in-person classes, do they have alternative resources?
- What impact will there be if staff rely on the LMS to provide testing?

Possible consequences:

- Delays in testing and/or instruction, whether in-person or online.
- Unable to reach class assignments or course content

Testing services

Regular non-instructional testing is typically performed online and may rely on either local or remote servers. These testing windows are usually set well in advance and have a significant impact on classroom schedules.

Questions to consider:

- Does online testing operate if the Internet is unavailable?
- What local systems are required for testing?
- What device management systems could impact student access to online testing?
- How long can you function without this service?
- What is the priority of this service compared to other services?
- What other systems might be impacted by the failure of this system?
- What are the critical testing systems the district relies on (e.g., state assessments, NWEA MAP, i-Ready, etc.), and what are their hosting environments (cloud vs. on-prem)?
- How do failures in other systems (e.g., internet outages, authentication systems) impact testing systems?

- Have we reviewed the vendor's uptime guarantees and responsibilities for restoration of service? Is there an existing Service Level Agreement (SLA)?
- What is our **backup plan** if a testing platform is unavailable during a high-stakes testing window?
- Do we have a **communication plan** for notifying staff, students, families, and state testing coordinators in the event of a disruption?
- What are our options for **make-up testing**, and how do those align with state or vendor policies?
- Do we have **offline contingency access** to student login credentials and rosters in case our SIS or authentication system is down?

Possible consequences:

- Delays or disruptions in testing may impact student performance on state-mandated testing.
- Disruption of high-stakes testing windows, potentially violating state or federal mandates and affecting student accountability measures.
- Loss of student testing data, leading to invalid results, the need for re-testing, or compromised instructional decision-making.
- Increased stress and confusion for students, educators, and administrators-especially during time-sensitive testing periods.
- Damage to district credibility with parents, state agencies, and testing vendors due to perceived lack of preparedness.
- Extended instructional downtime, as devices and staff time are diverted to rescheduling and recovering from the outage.

Finance, HR and Payroll Systems

This is the system(s) used to manage employee payroll, bill payments and HR data.

Examples

Finance, HR and Payroll Systems (ERP)

General questions to consider during or before a disruption

- What specific functionalities of the ERP system are affected by the cyber incident?
- Which ERP functions are critical for our district's operations?
- Is the ERP system cloud-hosted?
- What other systems or processes depend on the ERP system?
- What are the potential consequences of these dependencies failing?
- How often are backups performed, and where are they stored?
- Are backup procedures automated and regularly tested?
- How quickly can you recover data in the event of a system failure?
- Do you have redundant systems in place for critical components of our ERP system?
- What support do you receive from our ERP vendors during a disruption?
- Do our vendor agreements include adequate disaster recovery and continuity clauses?
- What regulations and standards must you comply with (e.g., FERPA, state regulations)?
- How long can you function without this service?
- What is the priority of this service compared to other services?
- What other systems might be impacted by the failure of this system?
- Are you prepared to hold school when the ERP system is not available? What other options are available?

Possible consequences

- Delayed or missed employee payroll, impacting staff morale, trust, and potentially violating labor laws.
- Inability to process financial transactions, including vendor payments, budget transfers, and purchase orders, disrupting district operations.
- Exposure of sensitive employee and financial data, leading to potential identity theft, legal liability, and mandatory breach notifications.
- Loss of real-time financial oversight, hindering leadership's ability to make informed budgetary decisions or respond to emergencies.
- Extended recovery efforts and potential audit findings, requiring significant time, resources, and possibly triggering compliance or insurance reviews.

Most common critical systems | Special considerations | Specific systems

None currently identified

Appendices

Critical Functions Checklist

☐ [Communication Systems](#)

- ☐ Email
 - ☐ Internal email
 - ☐ External email
- ☐ Phones
 - ☐ Classrooms
 - ☐ Elevator
 - ☐ Offices
 - ☐ Pool
 - ☐ Internal vs. External
- ☐ Faxing
- ☐ Public Announcement System
- ☐ Emergency Notification System
- ☐ Mass Notification platform for parents and staff
- ☐ Website
- ☐ Social Media Outlets

☐ [Facilities](#)

- ☐ Door/Access Control System
- ☐ Video Surveillance System
- ☐ HVAC
- ☐ Fire suppression
- ☐ Fire Alarm System
- ☐ Lights
- ☐ Visitor logging/management
- ☐ Exterior electronic public signage

☐ [Food Services](#)

- ☐ Food Services System
- ☐ Food delivery
- ☐ Computer/Tablet to access Food Services System (e.g. Point of Sale devices)

☐ [Network Services](#)

- ☐ Internet access
- ☐ Local network access
- ☐ Web content filters
- ☐ Access to ISD or other partner districts
- ☐ Firewall
- ☐ Remote Access
- ☐ Access to cloud-hosted services (e.g. Google, AWS, Azure)

- ☐ DNS
- ☐ DHCP
- ☐ Authentication systems
- ☐ [Transportation](#)
 - ☐ Special Education transport services
 - ☐ All route management systems
 - ☐ Dispatch system operational
 - ☐ Computer to access dispatch system
- ☐ [Student Services](#)
 - ☐ Student information Systems
 - ☐ Computer to access SIS system
 - ☐ Attendance tracking (manual or automated)
 - ☐ Learning management services (LMS)
 - ☐ Testing services
 - ☐ Classroom management/monitoring
- ☐ [Finance, HR and Payroll Systems](#)
 - ☐ Payroll
 - ☐ Check Run
 - ☐ Computer to access Finance system

Continuity of Operations Planning Worksheet

Function	Systems Inventory	Dependencies	Contingency Steps
Communication Systems			
Facilities			
Food Services			
Network Services			
Transportation			
Student Services			
Finance, HR and Payroll Systems			

Glossary

Term	Definition
Virtual / Virtualization	Technology that allows one physical computer to run multiple "virtual" computers at the same time. It helps districts make the most efficient use of their hardware by having one device do the work of many.
Authentication / Authentication Services	The process a system uses to confirm you are who you say you are before letting you in (e.g., checking your username and password).
DNS (Domain Name System)	Think of this as the "phonebook" of the internet. It automatically translates easy-to-remember website names (like google.com) into the numerical addresses computers use to connect to each other.
DHCP (Dynamic Host Configuration Protocol)	A service that automatically gives each device a unique address when it connects to the network, so IT staff don't have to set up every single phone, computer, or tablet manually.
MFA (Multi-Factor Authentication)	A security method that requires more than just a password to log in. It typically asks for something you know (your password) and something you have (like a code sent to your mobile phone).
Cloud / Cloud-hosted	Instead of running software on servers located in the school building, the software and your data are stored and managed by a

Term	Definition
	third-party provider and accessed over the internet.
Interdependencies	The way different systems rely on each other to work. It describes a "chain reaction" where the failure of one small part can cause problems for many other, seemingly unrelated systems.
Firewall / Content Filter	Digital gatekeepers that monitor traffic moving in and out of the district network. They are designed to block unauthorized access (Firewall) and restrict access to inappropriate or dangerous websites (Content Filter).
SLA (Service Level Agreement)	A formal contract or agreement between the school district and a technology vendor that defines the expected quality, availability, and support standards for a service.
ERP (Enterprise Resource Planning)	A comprehensive software suite used to manage all core business operations—such as finance, HR, payroll, and purchasing—in one integrated system rather than using separate, disconnected tools for each.