CONTINUITY PLANNING GUIDE & CHECKLIST

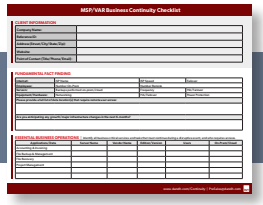
Establishing a comprehensive Continuity plan, along with proper training and testing, will enable you to safeguard your clients' operational resiliency during a disaster or unexpected event. Identifying business roles and processes, establishing lines of communication, implementing proper security measures, and assigning necessary hardware will generate ongoing best practices to ensure an inclusive continuity strategy.

Continuity planning should be included in the overarching IT plan of all organizations and reviewed on a regular cadence. This will ensure all documentation, hardware, software, etc. stays current as technologies and processes are updated to meet the organization's evolving needs and structure.

D&H

THIS GUIDE highlights key areas to focus on when developing a Continuity plan for your clients. When structuring continuity plans, it is an absolute must to consider local/state/federal compliances based on your clients' respective industry – (HIPAA, PCI, CIPA, etc.) – and reference those regulations throughout the planning/discussion phases. If your customers don't need specific industry compliances, another good resource to stay current on security standards and practices is the National Institute of Standards and Technology recommendations (www.NIST.gov).

Additionally, leverage our MSP/VAR Checklist for help compiling requisite information for each project to get your installs moving quicker.


MSP/VAR Business Continuity Checklist

THIS GUIDE IS NOT INTENDED TO REPLACE COMPLIANCY GUIDELINES WITHIN SPECIFIC INDUSTRIES (PCI, CIPA, HIPAA ETC), IT IS MEANT AS A SUPPLEMENTAL GUIDE ONLY

STEP 1 | Data Access & Control

Have your client define the processes and functions for each of their employees. Once correctly profiled, you are able to apportion employee access as well as the needed applications, data, and files that are crucial for their day-to-day functionality while working remotely.

- Endpoint Protection (intrusion/malware/anti-virus)
- VPN Client
- Remote Device Management

WORST-CASE-SCENARIO: Expired anti-virus software and a ransomware attack on a remote employee's device exposed patient records at a medical facility. The employee failed to share this breach with the IT department, causing HIPPA-related data vulnerabilities, downtime, and extensive damage to the practice's reputation.

STEP 2 | Data Security & Control

Remote access to the network helps clients work but it is crucial to develop a strategy that protects your client's employees, business and customers from a critical security breach. Global privacy regulations, escalating data losses, explosive personal data growth, and customer expectations have combined to make data privacy a business imperative. Ensure that your clients understand that taking the time to account for these security measures and risks upfront can ultimately pay for itself in preventing a single malicious incident. Maintaining proper security standards will keep their data safe and grant everyone peace of mind during challenging times.

- Encryption (Data and Email) – connection to network or to specific data
- Multi-Factor Authentication
- Risk Assessment
- Security Awareness Training

BEST-CASE-SCENARIO: Multi-Factor Authentication paid off for one construction company when IT received multiple notifications of attempted access to one of their financial email accounts. While the email password had been compromised, the hacker was unable to break into their system due to the additional MFA security layers.

STEP 3 | Data Backup & Retention

Backups are widely agreed upon to be essential to Continuity plans. Without access to files, businesses leave themselves vulnerable to losing large portions of their work. The methods, frequency, and retention standards often vary by company and industry. There are several types of backups ranging from full system backups and file-level backups to database-level backups. Each method has its own purpose and benefit.

BEST-CASE-SCENARIO: All project drawings are required to be saved in an archived database for one architect firm. As the lead Architect was reviewing past sketches, the folder was accidentally deleted, not being realized until months later. Luckily, the IT team was able to recover the old drawings through file-level backups without the need to restore the entire server.

STEP 4 | Network Access & Client Devices

Service disruptions, ranging from Internet outages to server crashes, require proactive recovery plans. Will your client need an automated recovery process or can the business manage with a manual recovery process for each disruption? Additional considerations should be made for employees that have bandwidth limitations, are working on a home network or do not have Internet access.

Ensuring that appropriate hardware is available for each remote employee is paramount. This hardware could consist of client devices and accessories such as laptops, docking stations, monitors, keyboards, mice, printers, headsets, phones, etc. Consider anything that will make the remote office as productive and comfortable as the on-site one, such as: client devices and accessories such as laptops, docking stations, monitors, keyboards, mice, printers, headsets, phones, etc

BEST-CASE-SCENARIO: During a tech firm's corporate office move, departments were given staggered work-from-home schedules to minimize office congestion. IT was not only able to proactively address potential remote workforce issues such as VPN access and risk of overload, but the drill acted as a best practices scenario in which a continuity plan emerged. Months later, COVID-19 hit; the firm's 1,000 employee workforce was able to transition from on-site to on-line within a matter of days.

BEST-CASE-SCENARIO: A decline in student's online presence was addressed by a cyber charter school. Not realizing the inability to complete work or be present for online classes was due to unreliable Internet connections, the school's administration proceeded to send "notice of absence" to parents. After further school review, the problem was alleviated and IT issued students mobile hotspots to help drive attendance and productivity.

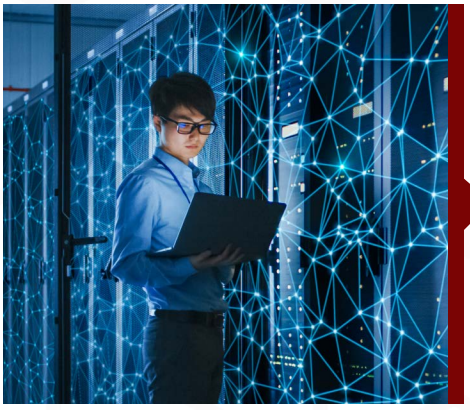
STEP 5 | Unified Communication & Collaboration

Leveraging UC and collaboration technologies such as messaging, video chat, conferencing and content sharing are all key elements in how businesses engage their employees and their customers through times of operational disruption. No matter the industry, your clients can create a digital customer experience with human engagement at the center with the right tools. At the same time, this rapid expansion of collaboration platforms cannot come at the expense of compliance requirements, and must be implemented and maintained to comply with industry standards.

BEST-CASE-SCENARIO: An insurance agency implemented personal and group cloud storage. This enabled their employees to collaborate remotely with just an Internet connection, no need for a VPN.

WORST-CASE-SCENARIO: A medical facility connected their main office and all smaller branch offices utilizing VoIP. Unfortuntaely, whenever their ISP conducted general maintenance (planned or emergency) at the main branch, all phone systems crashed at the branch offices as well. Effective implmentation is essential, in this instance, they should have implemented a cloud-based solution.

STEP 6 | Testing/Scanning Systems



TEST-TEST-TEST!!! Validate successful backed-up jobs, hardware and licensing capabilities, Internet connection bandwidth, and company-wide remote access. Stress-testing your client's infrastructure places the system under an intense workload to simulate a worst-case scenario; if a component crashes, hangs, or otherwise fails a dedicated stress test, there's a good chance that it won't be reliable under a heavy everyday load. Some parts of a continuity plan will be easier to test than others. For areas that are difficult to physically test, consider paper-based exercises and meetings to review and assess the plan. Also be aware that because of industry standards, your clients may be legally required to provide training and conduct drills to test the health and safety aspects of a plan, such as fire evacuation plans, handling of hazardous materials, special equipment, or otherwise operating in risky environments.

BEST-CASE-SCENARIO: Thanks to a system success/fail notification, a technician realized that his virtual machine backup was successful, but corrupt. The backup was fixed and validated immediately. Six days later, the organization's servers crashed. Without the planning/testing actions made by the technician, the last usable back up would have been over six-months old, translating to a complete loss of data for that timeframe.

STEP 7 | Set Expectations of Privacy

Ensure that your clients are including privacy clauses in their employee handbooks. The goal is to allow employees to work remotely without having their privacy invaded, but still allow the employer to monitor and track progress and productivity.

Continuity plans are living documents. Testing the fundamentals of the plan regularly will help evaluate how reliable it will be if and when a response to an incident or crisis is required.

Continuity plans should be evaluated and updated at least once a year. As well as when changes occur in the organization, the industry or the location the organization operates in.

Keeping staff up to date with plan changes will help them put it into action in case of an incident, which will in turn reduce the impact to the business.

Our exclusive SMB and K12 Partner Resource Guides are imperative in providing a seamless transition from on-site to on-line working and learning. Download at www.dandh.com/Continuity

BUSINESS CONTINUITY

A well thought out Business Continuity plan can mean the difference between an organization's survival or failure if disaster strikes. It becomes the cornerstone in minimizing operational interruptions in order to continue providing products and/or services, while mitigating financial loss.

EDUCATION CONTINUITY

Education Continuity in the event of a prolonged school closure is undeniably a critical component of school emergency management, as it promotes the continuation of teaching and learning despite circumstances that interrupt normal school attendance for one or more students.

Business Continuity: Planning Now & for the Future

Join Chris Phillips for a discussion on business continuity planning, a simulated business continuity plan development call with an SMB, and a review of the importance of each step of the process.

Visit www.dandh.com/SolutionsLab

MSP/VAR Business Continuity Checklist

CLIENT INFORMATION

Company Name:	
Reference ID:	
Address (Street/City/State/Zip):	
Website:	
Point of Contact:/Title/Phone/Email:	

FUNDAMENTAL FACT FINDING

Internet:	ISP Name	ISP Speed	Failover
Employees:	Number On-Prem	Number Remote	
Servers:	Backups performed on-prem/cloud	Frequency	HA/Failover
Equipment/Hardware:	Networking	HA/Failover	Power Protection
Please provide a full list of data location(s) that require remote user access:			
Are you anticipating any growth/major infrastructure changes in the next 6-months?			

ESSENTIAL BUSINESS OPERATIONS | Identify all business critical services and tasks that must continue during a disruptive event, and who requires accesss.

Applications/Data	Server Name	Vendor Name	Edition/Version	Users	On-Prem/Cloud
Accounting & Invoicing					
File Backup & Management					
File Recovery					
Project Management					

DAY-TO-DAY TOOLS | Prioritize the functions and resources required for continued productivity.

Platform	Server Name	Vendor Name	Edition/Version	Users	Notes
CRM					
Email					
Instant Messenger					
Meeting/Collaboration					
UCaaS/VOIP					
Collaboration/Productivity Suite					

INFRASTRUCTURE | Guarantee secure remote client access to network servers and affiliated data.

Physical/Virtual Server	Server Name	CPU Count	RAM	Total Storage Capacity (GB)	Amount of Storage Used (GB)	Operating System

SECURE, RELIABLE CONNECTION

Step 1: Ensure access to core applications and storage.
Step 2: Perform security risk assessments around specific threats where possible.

Applications	Server Name	Vendor Name	Edition/Version	Notes
VPN Client				
Cloud Based SSL				
Certificate Based Connection				
Soft Phones				
Home Internet Speed				

REMOTE MANAGEMENT | Determine the need for off-site data storage and backup.

Additional Notes	Notes
Current Software	
Personal or Corp-Issued Devices	
Means of Device Settings Manageability	

HARDWARE | Conduct an asset inventory to determine and document corporate-issued remote components.

Hardware	Vendor Name	Quantity	Existing or Needed
Displays			
Mouse			
Keyboard			
Headset			
Docking Station			
Cables			
Printer/Multifunction			
Webcam			

CLIENT DEVICES | Once computing devices are identified, determine what measures should be taken to protect and recover them.

Hardware	Vendor Name	Quantity	Existing or Needed	Endpoint Protection
PC				
Laptop				
Chromebook				
Tablet				
Phone - Apple/Android				

ADDITIONAL NOTES