Business Continuity Planning Checklist

Response and Recovery for Public Health Issues

BUSINESS CONTINUITY PLANNING CHECKLIST
Response and Recovery for Public Health Issues

This is an abbreviated checklist based on recent experience and lessons learned in executing a Business Continuity Plan (BCP).

Key Messages:

1. Establish a Crisis Management Team and a cadence for meetings.
2. Identify critical priorities for clients.
3. Develop communication plan for employees, clients, and partners.
4. Determine key data and reports needed to track the status of the situation and inform next steps.

Planning Outline:

Leadership

- ☐ Establish a Crisis Management Team, representing all relevant geographies and functions.
- ☐ Set a cadence for meetings based on the level of severity (once or twice a day in more serious scenarios).
- ☐ Report the latest key data points (people in the office, productivity levels, etc.) at the start of every meeting to determine your status and next steps.
- ☐ Decide how information from these meetings will cascade throughout the organization.

Communications

Internal communications
- ☐ Establish protocols for employee communications (email, text message, or other options).
- ☐ Ensure your managers have updated employee contact information.

Client communications
- ☐ Determine how, why, and when you will communicate with clients.
- ☐ Work in partnership with clients, seeking feedback on meeting their needs.

External communications
- ☐ Have a media response plan with an identified spokesperson and media statements.
- ☐ If you have an active social media presence, consider how it can be used to facilitate communications.
- ☐ If you have scheduled social media posts or marketing emails, consider if they are still appropriate in the BCP scenario.
- ☐ Identify your key business partners and vendors and what/how you need to communicate with them.

Employee Safety

- ☐ Provide continual updates to employees, including guidance on their daily commute and travel advisories.
- ☐ Work with public health officials and follow their guidelines.
- ☐ Have an office sanitation procedure and auditing/reinforcing process. Clearly outline cleaning standards, describing the frequency, cleaning product (alcohol-based), and areas needing cleaning (any surface where hands might come in contact).
- ☐ Provide necessary protection to all employees such as face masks, sanitizing products, and tissues. Also consider having a non-contact thermometer in the office.
- ☐ Designate a role to collect and report employee health data.
- ☐ Communicate clear guidelines on when employees should stay home. In an outbreak situation, remote work is the most effective way to protect employees and recover business operations.
- ☐ If your offices have to shut down, take a phased approach when bringing employees back in order to test your safety procedures and not overburden your admin team.
- ☐ Provide safety tips to employees. According to the World Health Organization, the best precautions to take, in order of efficacy are:
  1. Wash your hands regularly with soap and water, scrubbing for 20 seconds.
  2. Avoid close contact—less than 3 feet—with individuals who are coughing or sneezing.
  3. Avoid touching your face.
  4. Cough or sneeze into your elbow or a tissue, not your hands.

Workload Management

- ☐ Identify workload priorities from a client's perspective. When necessary, confirm those priorities with clients.
- ☐ Identify where gaps exist in delivering service to clients on critical tasks.
- ☐ Assess priorities and available team members to balance resources and critical workloads.
- ☐ Ask managers and supervisors to focus on workload management and provide employees with task priority.
- ☐ Review your productivity metrics and revise them for the BCP situation.
- ☐ If current productivity tracking doesn't work in a remote situation, use manual productivity tracking or data gathering processes, even if that means using Excel or emails at first. Launch this to employees as soon as possible and make incremental improvements to the process daily.
- ☐ Ensure business leaders work closely with the technology team to avoid any tech-based interruption.

Technology

- ☐ Set up and test remote access for employees.
- ☐ If you already have a work-from-home policy, expand the capacity of your server to allow more remote access without sacrificing too much connection speed.
- ☐ Back up on-premise applications and services you rely on (like Windows File Share drives and agency management systems) with cloud-based applications that can be accessed remotely.
- ☐ Survey your employees on their work-at-home technology abilities so you can plan how many people can work at home and what gaps you have for a work-at-home strategy (e.g. quality of their home internet, number of monitors).
  - ☐ Based on your enterprise risk management principles, decide if employees working at home will be using equipment provided by the company or their home equipment. Depending on the decision, your risks and planning may vary.
  - ☐ Follow security best practices, ensuring that home computers have:
    - ☐ Latest anti-virus and malware software with newest updates
    - ☐ Latest Windows Update patches, and Windows 10 is preferable.
  - ☐ Ensure that remote desktops (e.g. Citrix/Remote Desktop/VDI) have:
    - ☐ All applications that a remote employee would need to conduct priority tasks.
    - ☐ Encryption enabled.
    - ☐ Disabled Terminal Services remote printing and remote file access for improved security.
- ☐ Test how your phone system can work for remote access.
- ☐ Set up a publicly accessible file-sharing repository to ensure employees can access company documents (e.g. Microsoft's SharePoint).
- ☐ Summarize your information security practices and policies for work from home and reinforce it with your employees frequently.