The following documents listed below have been compiled from our exhaustive list of Business Continuity & Disaster Recovery Planning/Contingency Planning (BCDRP/CP) packets for purposes of providing an overview of the depth and details of the material we've developed.

For additional samples, please email us at info@flank.org

Section II: Roles and Responsibilities

A "Team Effort" Approach

Having clearly defined roles and responsibilities is essential to the plan's success, and while relevant information is to be completed with Appendix K for the alternate site(s), it is also important to provide detailed information on these very roles and responsibilities for all in-scope personnel for the entire plan lifecycle. Having such roles and responsibilities defined and well-documented ensures that a team effort approach takes root in which all employees are working together for creating a successful plan.

The following roles and responsibilities are to be assigned to relevant personnel within [company name]:

BCDRP/CP Lead Authority

The BCDRP/CP Lead Authority is ultimately responsible for coordinating, facilitating, and guiding the entire BCDRP/CP process, from beginning to end. Such an individual is the true decision-maker and the ultimate authority on all critical BCDRP/CP decisions. Specifically, this/these individual(s) is/are responsible for the following:

- Guiding and overseeing the entire BCDRP/CP process.
- Be the one true single point of contact for the organization.
- Make decisions based on the actual needs of the organization.
- Report upstream to senior management on a regular basis during the entire BCDRP/CP process.
- Delegate to subordinates all essential roles and responsibilities as necessary.
- Essentially organize and supervise all personnel and coordinate all activities.

Name	Title	Email	Contact Phone #1	Contact Phone #2

BCDRP/CP Facility Personnel

The BCDRP/CP Facility Personnel are an incredibly important component of the entire BCDRP/CP process, as they are chiefly responsible for the day-to-day operations of the facility, and will also be responsible for the same day-to-day operations at the alternate business site(s). Specifically, this/these individual(s) is/are responsible for the following:

- That the alternate business site(s) are in good working order, that they have all technical, security, and operational resources on hand to perform the duties necessary for [company name].

- That adequate provisions are in place regarding housing, transportation, and food.
- That all necessary procedures are underway for removing all assets from the facility that have been damaged, and doing what is necessary for preserving – if possible – such assets, while also mitigating – to the fullest extent possible – any further damage to the facility.
- That all resources have been procured and are onsite at the alternate business site(s) so that [company name] can commence with operations.
- Working with all organizations (i.e., local, state, federal authorities, agencies, along with contractors, etc.) in assessing damage done to facility, but also for coordinating necessary re-build efforts to the facility.

Name	Title	Email	Contact Phone #1	Contact Phone #2

BCDRP/CP Information Security Personnel – Networks & Related Systems

BCDRP/CP Information Security Personnel for Network & Related Systems are instrumental in a number of ways. First and foremost, they are vital for helping put in place an acceptable network at the alternate business site(s) for meeting the information security triad of Confidentiality, Integrity, and Availability (CIA). Without such personnel, communication and other forms of business operations would not be possible. As such, this/these individual(s) is/are responsible for the following:

- Design/architect, configure and implement a network (i.e., Local Area Network – LAN; Wide Area Network – WAN) at the alternate business site(s). The term "network" essentially means the following:
  - Communications equipment (i.e. phone, phone lines, cabling, wiring, etc.)
  - Hardware and supporting software (i.e., VOIP communications, firewalls, routers, switches, load balancers, server boxes, etc.)
  - All other necessary "network" assets deemed vital for continuation of operations
- Ensure a phased approach is taken when deploying network assets based on priority and overall need for the organization at the alternate business site(s).
- Build and deploy any other necessary "network" assets.
- Collaborate as necessary with BCDRP/CP Information Security Personnel for Servers/Applications & Related Systems Personnel.
- Eventually, assist in re-building, re-configuring, and re-deploying the network at the primary facility.

Relocation Strategy and Alternate Location

Should a disaster take place that results in [company name]'s facilities (i.e., offices, etc.) unable to be occupied because of physical/environmental constraints, then alternate sites are to be identified and used for relocating all relevant personnel. The term "relevant" implies all personnel that are essential to the plan, and ultimately, essential to re-establishing operations for [company name]. As such, authorized personnel are to complete **"Appendix H – Alternate Business Sites"** Matrix.

Recovery Plan Initiatives

Numerous recovery plan initiatives are to be in place for ensuring [company name] can recover – as best as possible – from a disaster and/or business interruption. Having documented recovery steps in place will further aid and facilitate the entire process of the plan for [company name]. The core initiatives of the recovery plan include the following:

- Measures to enact during or immediately after a disaster.
- Activating the plan as necessary due to a disaster.
- Initiating alternate business site protocols.
- Undertaking necessary initiatives for returning operations to the primary site(s).

Specifically, each of the aforementioned initiatives are to consist of the following processes and procedures.

A. Initial Measures to Enact

The following emergency response measures are to be enacted – as necessary, and when/where applicable – during or immediately after a disaster:

- Evacuate all personnel from all facilities for which the disaster has affected. Human life is always the top priority for any type of disaster which may affect the organization.
- Notify all personnel with all forms of available communication, such as, but not limited to, the following: email, loud-speaker/PA/announcement forums, verbal communication to other individuals or group, cellular phone calls, calls to landlines, office extensions, etc.
- Formally produce a documented Assessment of Damages to the organization, for which such information is to be dispersed to all relevant parties. Thus, complete the **"Appendix I – Assessment of Damages"** form.
- Formally declare that a disaster has taken place. This is to include contacting all relevant parties as necessary for issuing such a declaration.

B. Notification to Management and Relevant Third-Parties

The following notification measures are to be enacted – as necessary, and when/where applicable – during or immediately after a disaster:

- Notify all senior management (i.e., C level officers), and other in-scope personnel of the current disaster and what steps are being taken.
- Notify all relevant third-parties (i.e., suppliers, vendors, etc.), and other in-scope personnel of the current disaster and what steps are being taken.

- Complete the **"Appendix J – Third Party Organizations"** Matrix.