****

**BUSINESS CONTINUITY MANAGEMENT POLICY**

Effective contingency planning can minimize the impact of a disaster or threat. This document provides planning and program guidance for implementing a Business Continuity Plan (BCP). 17 Pages 20-685

**We strive to continually update our efficiency library for the benefit of our members.  Please consider contributing documents from your organization.**

**Thank you!**

These documents have been voluntarily contributed by NOREX members with the full knowledge that other members may use them in any manner they see fit. NOREX and its members shall not be held liable for any statements or interpretations contained within the documents.

**Company’s Business Continuity Management Program Policy and Procedures**

**Last updated:**

1. **Purpose, Scope, Situations, and Assumptions**
2. Purpose

This document provides planning and program guidance for implementing Company’s Business Continuity Plan (BCP). In addition, it includes the program to ensure that Company is capable of conducting its main business functions under the possible threat of disruptions. While prediction of the severity and consequences of an emergency is not exact, effective contingency planning can minimize the impact on Company’s responsibilities. The ability to maintain critical services is of the utmost importance.

1. Scope

This Business Continuity Plan applies to all of the functions, operations, and resources necessary to ensure the continuation of Company’s critical business functions in the event of a disruption of normal operations. Company’s staff members must be familiar with continuity policies and procedures, and their respective continuity roles and responsibilities.

For Company’s Business Continuity Plan, the following applies:

1. Perform maintenance of the plan on a continual basis.
2. Test the Plan periodically. NOTE: The recommendation is to test the Plan annually.
3. Review the Plan with individual teams and new employees.
4. Review the Plan after any major changes have happened in the organization, e.g., major employee change, changes in upper management, growth or loss of departments, changes to the disaster recovery plan, changes to the emergency response plan, etc.
5. Assumptions

The basis of the development of the Business Continuity Plan involves the following requirements.

1. General Requirements
2. Within twelve (12) hours from the time of the activation of the Continuity Plan, the Recovery Teams and essential staff members will need to be able to support the continuation of Company’s critical business functions via available communications and information systems. Affected departments should be contacted and proper assessments should be made at this time to determine if personnel need to relocate or if the current situation is sufficient enough to facilitate this requirement. During this time the scope of the disaster should be evaluated, and the organization should be able to inform the departments of the timeframe for the disaster.
3. The documentation of Company’s detailed daily operational procedures does not display in this Plan. Each department is responsible for their own documentation of any procedures that are critical to their daily operations. Upon completion of this documentation, and for any subsequent updates of the document, these procedures should be stored in a secured off-site location, or in a tool provided for cloud computing. Employees who notice anything that could cause a disruption in service such as fire, an explosive device, flooding, or malicious code, he or she should notify someone immediately. At this time, we will respond to the incident based off the Emergency Response Plan or decide if the Business Continuity Plan should be activated.
4. All critical resources should be listed in the Plan and be available for viewing. These resources can derive from other business partners.
5. The provision of the need for a proper facility and supporting resources will be available based upon the importance of the business function to support a timely recovery.
6. An emergency condition may require that the Recovery Teams and essential staff members relocate to the continuity facility, or to their telecommuting sites.
7. Operating Requirements

Upon notification of an emergency, the following applies:

1. BCP leads must report to the predetermined alternate site as directed by management.
2. Management personnel must maintain their normal lines of authority, which includes the reporting structure, and at all times must act as a Team Member or Leader when appropriate.
3. All personnel participating as Team Members must keep informed of the latest emergency developments and complete their responsibilities as defined in the plan. Deviations from the Plan are only acceptable if approved by a Leader of the Continuity Plan.
4. Essential staff must keep informed of the latest emergency communications and any Plan changes or improvements. It is the responsibility of the staff member as well as the BCP Lead, to check in with essential staff periodically even if no new information is available.
5. BCP Team Members have the responsibility to share their expertise as needed in any of the four (4) phases of operations, which include the following:
	1. Phase I: Readiness and Preparedness
	2. Phase II: Activation and Relocation
	3. Phase III: Recovery Operations
	4. Phase IV: Reconstitution

NOTE: all communication about a disaster will be through phone conversations, text messages and company email which is cloud driven and unaffected by the state of the data center.

1. **Organization and Assignment of Responsibilities**

This section identifies the key staff member positions within Company. These positions include the following: essential staff members, continuity team members, those identified in the order of succession and delegation of authority, the Recovery Team Leader, and others who possess additional continuity responsibilities. The following delineates these key essential staff members:

1. Initial Response and Containment

The BCP leads and the communication team will need to manage the immediate message and fall out of a disaster as soon as it happens. The communication team will be responsible for notifying the essential staff of the disaster and the current situation so they can begin to work with their individual departmental BCPs to be able to support the organization. The BCP leads will work to identify the issue, the extent of the disaster, and determine if partial or complete functionality is lost. This initial information will allow the departmental BCP leads to be able to support the organization.

1. Essential Staff

Individuals are critical to the operations of any organization. Selecting the right people for an organization’s staff members is vitally important, and this is especially true in a crisis. Leaders set priorities and keep focus. During a continuity event, the activation of emergency employees and other special categories of employees allow these individuals to perform assigned response duties. One (1) of these categories is the essential staff members. In respect to essential staff, Company must complete the following:

1. Identify and designate essential staff as those positions and personnel that they judge to be critical to the organization’s operations in any given emergency. **NOTE**: The Business Continuity Liaison maintains a roster of continuity positions.
2. Identify and document that essential staff members possess the skills necessary to perform critical business functions and supporting tasks. **NOTE**: The Business Continuity Liaison maintains a roster of essential staff members.
3. Officially, inform all essential staff members of their roles or designations, to ensure they know and accept their roles and responsibilities.
4. Ensure that essential staff members participate in the organization’s continuity Test, Training, and Exercise (TT&E) program. **NOTE**: The Business Continuity Liaison maintains training records.
5. Provide guidance to essential staff members concerning individual preparedness measures to ensure response to a continuity event.
6. Non-essential staff may be needed based on the evaluation of the disaster. When the disaster is evaluated the downtime will determine if the essential staff can maintain business functions until the return of normal operations or if additional staff is required.
7. Teams

Essential staff memberswill be defined by departments to help facilitates Company’s recovery efforts. This organization depends on its departments to be able to independently operate and maintain their responsibilities through the disaster depending upon the nature and scale of the disruption. Each department has an individual departmental BCP that will guide them through a BCP scenario. The departmental BCP will designate essential staff and department need. Essential staff members are responsible for organizing their department’s recovery efforts and reporting progress back to the BCP teams. They will also help identify any additional needs for the department during a disaster. **NOTE**: The purpose of this plan is not to detail the daily use of existing standard operating procedures, which is the purpose of the individual department BCPs.

To assist the teams, the following key individuals complete their specified roles:

1. The Business Continuity Plan Liaison coordinates the relocation of essential staff members to other worksites in an emergency.
2. Communication Team, in conjunction with advisement from the reporting structure outlined in Company’s Emergency Response Plan, informs the agency as a whole of current safety issues and general status in regard to an incident that could impact business and personnel wellbeing. They provide location access and associated resources as well as overarching communication needs to the agency.
3. The Recovery Team is responsible for maintaining the recovery procedures and coordinating the recovery of Company’s business functions and processes.
4. In addition, continuity operations may require support from other agencies and commercial vendors.

Identification of Company’s team details, as well as external agency and vendor contact information, will be found in individual department plans.

1. All Staff

It is important for Company to keep all staff members informed and accounted for during a continuity event. This includes the identification of non-essential staff members for recovery operations. The Communication Team will make sure to update all staff via email. Individual members will be also be contacted via text or call. Essential staff members’ phone numbers will be listed in the departmental BCP(s).

1. Company employees must remain in contact with their supervisor during any facility closure or relocation situation.
2. Company must ensure that staff members are aware of, and familiar with, the Emergency Response Plan in order to communicate at an agency wide level during an emergency.

**The plans should support the crisis management timeline as illustrated in the diagram below:**

****

**BCP Teams and Members**

**BCP Team Leads**

Leader:
Leader:
Leader:
Leader:

**BCP Recovery Team**Leader:
Leader:
Leader:
Leader:

**Communication Team**Leader:
Leader:
Leader:

Leader:

**DR Recovery Team**Leader:
Network Engineer:

Voice Engineer:
System Recovery:

System Support:

Tech Support:

**Business Continuity Plan Liaison**

1. **Essential staff**

|  |  |  |  |
| --- | --- | --- | --- |
| **Department** | **Team/Role** | **Name** | **Contact** |
|  **\*\*\*Intention left blank for sharing purposes \*\*\*\***    |

1. **Security and Privacy Statement**
2. This Plan is For Official Company Use Only. This official use declaration is due to the following reasons:

**Note**: Portions of the Plan contain information that raises personal privacy concerns, which may affect the security of equipment, services, or other entities. These portions may be exempt from mandatory disclosure under the Freedom of Information Act (see 5 United States Code §552, 41 Code of Federal Regulations Part 105-60).

The following applies to the handling of the Plan:

1. The Plan must be controlled, stored, handled, transmitted, distributed, and disposed of with each new revision.
2. The Recovery Team Leader must provide prior approval for any release of the Plan to the public or to any other personnel.
3. Distribution of copies of the Plan will take place to other organizations as deemed necessary to promote information sharing and to facilitate a coordinated inter-organization continuity effort.
4. The Recovery Team Leader must provide approval for further distribution of the Plan.
5. The Team Concept of the Plan

The sections below describe how the Business Continuity Plan utilizes a team concept for recovery methodology to carry out each of the Plan phases.

This BCP’s purpose is to help guide the organization on how to handle itself through the disaster, however each department has its own BCP to oversee the responsibilities of the specified department. All required recovery actions are the responsibility of designated team members. Each team member reports to their Team Leader for coordination, but independently performs certain tasks and procedures that are required to restore and recover their area of responsibility. Each team member may call upon the appropriate personnel necessary to perform their responsibilities successfully. Employees on each team have operational duties within their own areas of responsibility. **NOTE**: The purpose of this Plan is not to detail the daily use of existing standard operating procedures, which is the purpose of the individual department BCPs.

The two (2) defining characteristics of the team concept approach are accountability and flexibility. During a disaster, some members may not be available at certain times, or others may not be aware of all necessary procedures to accomplish their mission. The team approach allows for the innovation of implementation, while keeping accountability as to required function. The same is true for the team providing the needed flexibility in a disaster, to complement available skills to handle the actual disaster situation.

The Teamwork site and file share is the living place for the document. Both are mission critical servers which will be backed up and running within four (4) hours of a disaster. Both of these sites can be accessed by the individuals deemed necessary. The Plan will also be kept on the devices of the liaison and BCP team members. Additionally, the Plan will be kept off site on the (location) file share with physical copies located in the (location) and (location) offices. The list of individuals to contact will be stored with this document in all locations.

1. **Phase I: Readiness and Preparedness**
2. Company must participate in the full spectrum of readiness and preparedness activities to ensure that personnel can continue critical business functions in an all-hazard/threat environment. The organization’s readiness activities apply to the following two (2) key areas:
3. Organization readiness and preparedness
	* + - 1. Company’s preparedness includes the organizations call tree and Company’s internal and/or external websites.
4. Staff readiness and preparedness
	1. Company’s essential staff members must keep a physical copy of the BCP and understand their responsibilities. They should take the BCP with them if relocated during an emergency. Vital Records Management
5. Vital Records Management

Vital records are an important part of Company’s business continuity resources, and a copy must be part of the BCP. Vital records refer to Company’s information systems, applications, electronic and hard copy documents, references, and records. They include the classified or sensitive data needed to support Company’s Critical Business Functions during a continuity event. Company must incorporate its vital records program into the overall continuity program, plans, and procedures.

1. Identifying Vital Records

Company must maintain a complete inventory of vital records. It is recommended that this inventory be maintained at a back-up/offsite location in a staging kit, to ensure continuity if the primary operating facility is damaged, destroyed, or unavailable. Each department should provide a complete inventory of vital records in the department plan.

Storage of the vital records in a packet, or collection, should include the following:

1. a paper copy or electronic list of Company’s key organization personnel and essential staff members with current telephone numbers
2. a vital records inventory with the precise locations of vital records [i.e., where is our co-location (COLO) located and what is located there]
3. necessary keys or access codes
4. listing of the access requirements and sources of equipment necessary to access the records
5. continuity facility locations
6. lists of experts to handle records for each department
7. a copy of Company’s Business Continuity Plan(s)

Company’s Business Continuity Liaison should review the vital records packet no less than annually to ensure the information is current and correct. An electronic copy of the business continuity solution will be made available to ensure that it is easily accessible to the appropriate personnel when needed.

**NOTE**: Although the Disaster Recovery Plan will ensure access to most of these vital record items, a staging kit is required in the event there is a need to have forms, checks, recording templates, or other financial instruments available.

1. Protecting Vital Records

The protection of vital records is essential to guarantee their availability to Company during a continuity event, which allows for the performance of Critical Business Functions. Assess the vital records and database risks to complete the following:

1. Identify the risks involved in retaining the vital records in their current locations and media in terms of their possible destruction, and then identify the amount of difficulty that would be involved to reconstitute these records.
2. Identify offsite storage locations and requirements.
3. Determine if alternative storage/media is available.
4. Determine the requirements to duplicate these records and provide alternate storage to provide easy access to the vital records under all conditions.

Identification of Company’s vital records displays in each department’s BCP.

1. Staging Kits

Staging kits are only necessary if there are vital records or any material that is needed in the event of disaster. A copy of records or the extra material should be placed in a staging kit at both the (location) and (location) office in order to be available to take in the event a disaster is declared.

1. **Phase II: Activation and Relocation**
2. Evaluation

For agency wide guidance on emergencies such as fires, bomb threats, flooding, etc., please reference the Company Emergency Response Plan (ERP). Anything outside of the ERP will have to be evaluated by the BCP team to determine the extent - of the disaster and the next steps.

The first step of this phase is to assess the damage to operations and determine if there is a need to utilize an alternate site. The notification for this extremely important decision will come from the CEO, President, COO, or BCP Leads. Upon notification of a disaster situation, there is an activation of the Recovery Teams, the notification procedures commence, and the business team(s) will report and be ready to relocate to the alternate location if necessary.

If a disaster is declared, the business Recovery Team completes the following:

1. Retrieve the calling tree information from the BCP, and call staff members to inform them of the event and next steps. Call external contacts to inform them of the event and known status of the event.
2. Contact team leads and/or BCP lead(s) regarding any issues related to the following:
	1. relocating to the recovery site or implementing additional remote workers
	2. arranging for access to enter the recovery site
	3. emergency procurement
	4. use of leave (HR&A and Diversity support)
	5. Workers’ Compensation
	6. compensation for injuries
	7. overtime pay
3. Notify team leads or BCP lead if an event or disaster may affect staff members with special needs.
4. Document the completion of these bulleted items noted above for use during and after an event has occurred.
5. Asset Recovery and Salvage

After BCP leads and building facilities staff confirm that it is safe to enter the buildings, the departments can send in their own staff members, considered Department Salvage Teams, who will identify which items (i.e., equipment, documents, etc.) are salvageable, and institute the necessary immediate actions. If items are salvageable, they will complete the following:

1. organize the working party of available staff members
2. collect items and place them in boxes/containers, while labeling the contents
3. move boxes to the recovery site
4. take an inventory of the contents of each box
5. prepare a list of items recovered
6. Setting up a Command Center

With the declaration of an evacuation of the primary site, and/or the declaration of a disaster, advisement of the chosen command center to team leaders and management personnel is required as outlined in the published Emergency Response Plan.

1. Relocation Process

Upon the activation of the Business Continuity Plan, the communication team advises personnel of this activation and essential staff members will relocate to the designated continuity facilities or to the telecommuting sites to perform critical business functions and other continuity-related tasks.

1. The implementation of emergency procedures during work hours (with or without a warning), requires the following:
2. Essential staff members (including Recovery Team personnel, if applicable) depart to the designated continuity facility, or to the telecommuting sites, from the primary operating facility or from their current locations.
3. Non-essential personnel, who are present at the primary operating facility, or another location, will receive instructions. In most scenarios, these individuals will be asked to proceed to their homes or other facilities to wait for further guidance. Additional information will be obtained by contacting the team lead who should receive updates and information from the communications team.
4. The implementation of emergency procedures during non-work hours (with or without a warning), requires the following:
5. Essential staff members (including Recovery Team personnel, if applicable) will deploy to the designated continuity facility from their current location(s).
6. Non-essential personnel will remain at their residence, or other designated facility, to wait for further instructions.

Non-essential personnel may be required to replace or augment essential personnel during activation. The Recovery Team will coordinate these activities with the replacement staff members on a case-by-case basis. Non-essential personnel will remain available to replace or augment essential staff members, as required.

The essential staff members or members of the Recovery Team may direct non-essential personnel to return home until further notice.

1. **Phase III: Recovery Operations**
2. Division Relocation Logistics
3. The Recovery Team will be first to arrive at the continuity facility to prepare the site for the arrival of the essential staff members and other teams. Upon arrival at the continuity facility, the Recovery Team will complete the following:
4. prepare check-in duty stations for the Recovery Team and essential staff member arrival
5. address telephone inquiries from the Recovery Teams, essential staff members, and from the non-essential staff members
6. retrieve the staging kits (if applicable)
7. perform other tasks as described in the contingency plan

As essential staff members arrive, the Recovery Team Leader will conduct an in-processing checklist to ensure accountability. In addition, there will be an identification of all available organizational leadership at the continuity facility.

1. Upon arrival at the continuity facility, the essential staff members will:
2. report immediately for check in and processing
3. receive all applicable instructions and equipment
4. report to their respective workspace as notified during the activation process
5. activate specialized systems or equipment
6. monitor the status of Company’s personnel and resources
7. continue critical business functions
8. prepare and disseminate instructions and reports, as required
9. comply with any additional continuity reporting requirements
10. Recovery team members should attempt to account for all essential staff personnel using one (1) or both of the following processes:
11. call trees listed in departmental BCP
12. email through accessing the web application of O365

NOTE: Non-essential staff should report to their team leads. Team leads are responsible for informing and tracking staff.

Company has designated the (location) location for its alternate site and has prepared essential staff members for the possibility of unannounced relocation to the site to continue performance of critical business functions.

1. Recovery Site Resources
2. Identification of the recovery site required resources are:
3. additional hardware such as computers and phones
4. places for essential staff to setup and conduct business
5. Recovery of Critical Business Functions

Departments will conduct an independent business impact analysis (BIA) to help identify and prioritize Critical Business Functions (CBF) that must continue during the time of a disaster. Business CBFs are a limited set of specific business functions that must continue throughout, or must rapidly resume after, a disruption of normal business activities. CBFs, as validated and approved by management, and listed in a table below. These tables include the Maximum Tolerable Downtime (MTD) for the CBF, as well as the Recovery Point Objective (RPO) for related data, and the Recovery Time Objective (RTO) for the supporting systems.

1. **Phase IV: Reconstitution Operations**
2. After confirmation from BCP lead(s) of an emergency relocation, the following individuals initiate and coordinate operations to salvage, restore, and recover the primary operating equipment after receiving approval from the appropriate State and local law enforcement and emergency services. This includes the following:
3. The designated Company Recovery Team leads (or who they designate) serve as the Reconstitution Manager(s) for all phases of the reconstitution process.
4. Each department subcomponent designates a constitution Point-of-Contact (POC) to work with the Recovery Team and to update office personnel on the developments regarding reconstitution and provide names of the reconstitution POCs to the Reconstitution Manager.
5. Reconstitution commences when the BCP lead(s) declares the end of the emergency. The reconstitution plans are viable, regardless of the level of disruption that originally prompted implementation of the Continuity Plan. After the appropriate authority determines the end of the emergency, which is coordinated with other State, local, and/or other applicable authorities, the implementation of one (1), or a combination of the following options, may occur:
6. Continue to operate from the continuity facility, which could include, or be solely from, telecommuters.
7. Reconstitute Company’s primary operating facility and begin to return to this facility in an orderly manner.
8. Begin to establish a reconstituted Company in another facility or at another designated location.
9. Company management develops procedures, as necessary, to re-assign staff members, if needed.
10. After verifying that the required capabilities are available and operational, and that Company is fully capable of accomplishing all critical business functions and operations at the new, restored facility, or via the use of telecommuters, the Recovery Team begins the following:
11. supervising a return of personnel, equipment, and documents to the primary operating facility
12. moving to a temporary or new permanent primary operating facility
13. The Stand down should also include hot and cold debriefs and documenting of lessons learned and an action plan for improvement.
14. **Plan Maintenance and Testing**
15. **Maintenance**

Each department lead, supervisor, or manager is responsible for maintaining his or her department’s Continuity Plan. As part of the maintenance of Continuity Plans and procedures, Company management reviews and updates the Continuity Plan at least annually from the date of publication. The Company Security Committee is responsible for providing guidance and facilitating the annual Plan reviews and updates. In addition, updates and modifications to the Plan occur when there are significant organizational, procedural changes, or other events that affect continuity processes or procedures. Comments or suggestions for improving this Plan can be directed to the Security Committee for review.

1. **Test, Training, and Exercises (TT&E) Program**

To support the organization’s preparedness and validate the continuity capabilities, program, and ability to perform critical business functions during any emergency, Company must establish an effective TT&E program. This testing, training, and exercising of continuity capabilities is essential to demonstrating, assessing, and improving the company’s ability to execute the continuity program, plans, and procedures, and for the following reasons:

1. Training familiarizes essential staff members with their roles and responsibilities in support of the performance of the organization’s critical business functions during a continuity event.
2. Tests and exercises serve to assess, validate, or identify the needs for subsequent correction of all components of a Continuity Plan’s, policies, procedures, systems, and facilities that are used in response to a continuity event. Periodic testing also ensures that the equipment and procedures are available in a constant state of readiness.

Company must perform TT&E events at regular intervals and log the actual dates in accordance with the table below.

*\*\*\*The Federal Department of Homeland Security provides guidance on performing and evaluating security exercises as part of the Homeland Security Exercise and Evaluation Program (HSEEP). See* [*https://www.fema.gov/media-library/assets/documents/32326*](https://www.fema.gov/media-library/assets/documents/32326) *for more information.*

1. **Record of the Company’s Changes to the Plan**

|  |  |  |  |
| --- | --- | --- | --- |
| **Section** | **Date of Change** | **Individual Making Change** | **Description of Change** |
|   |   |   |   |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Continuity TT&E Requirements** | **Monthly** | **Quarterly** | **Annually** | **As Required** |
| Test alert, notification, and activation procedures for all essential staff members. |   |   |  X |   |
| Test capabilities to perform critical business functions. |   |     | X   |     |
| Test plans for recovering vital records, critical information systems, services, and data. |   |     | X |   |
| Test internal and external interdependencies with respect to performance of critical business functions. |     |   | X   |   |
| Train essential staff on roles and responsibilities, |   |   | X |   |
| Conduct successor training for all organization personnel who assume the authority and responsibility of the organization’s leadership if that leadership is incapacitated or becomes otherwise unavailable during a continuity situation. |     |     |     |  X   |
| Train on the identification, protection, and ready availability of electronic and hardcopy documents, references, records, information systems, and data management software and equipment needed to support critical business functions during a continuity situation for all staff members involved in the vital records program. |     |     |     | X   |

1. **Authorities and References**
2. Emergency Response Plan

Company’s Emergency Response Plan is located on the company intranet, will be kept with the vital records, stored with the BCP and stored with the appropriate individuals.

1. **Glossary**
* **Activation** –Implantation of a continuity of operations plan, whether in whole or in part, it becomes “activated.”
* **All-Hazards** –The spectrum of all types of hazards, which includes the following: accidents, technological events, natural disasters, terrorist attacks, warfare, and chemical, biological including pandemic influenza, radiological, nuclear, or explosive events.
* **Alternate Facilities** – The locations, other than the primary facility, used to carry out critical business functions in a continuity event. “Alternate facilities” refers to not only other locations, but also to nontraditional options, such as telecommuting, and mobile-office concepts.
* **Business Continuity Liaison** - The BC liaison ensures that there is a plan for relocating the pre-designated essential staff members to other worksites in an emergency.
* **Business Continuity Plan (BCP)** Refer to the definition for Continuity of Operations.
* **Business Impact Analysis (BIA)** – A method of identifying the effect of failing to perform a function or requirement.
* **Business Process Analysis (BPA)** – A method of examining, identifying, and mapping the functional processes, workflows, activities, personnel expertise, systems, data, and facilities inherent in the execution of a function or requirement.
* **Communications** – The voice, video, and data capabilities that enable the leadership and staff members to conduct the mission critical business functions of the organization. Robust communications help ensure that the leadership receives coordinated, integrated policy and operational advice and recommendations and will provide the ability for governments and the private sector to communicate internally and with other entities (including with Federal agencies, State, territorial, tribal, and local governments, and the private sector) as necessary to perform their Division Critical Business Functions (DCBFs).
* **Continuity** – An uninterrupted ability to provide services and support, while maintaining organizational viability, before, during, and after an event.
* **Continuity Event** – Any event that causes an agency to relocate its operations to an alternate or other continuity site to ensure continuance of its critical business functions.
* **Continuity Facilities** – The locations, other than the primary facility, used to carry out critical Division functions, particularly in a continuity situation. “Continuity facilities” refers to not only other locations, but also nontraditional options such as working at home, telecommuting, and mobile-office concepts.
* **Continuity of Operations (COOP)** – An effort within individual agencies to ensure they can continue to perform their Mission Critical Division functions and Primary Mission Critical Division functions during a wide range of emergencies, including localized acts of nature, accidents, and technological or attack-related emergencies.
* **Corrective Action Program** – An organized method to document and track improvement actions for a program. The Corrective Action Program (CAP) system is a web-based tool that enables Federal, State, and local emergency response and homeland security officials to develop, prioritize, track, and analyze corrective actions following exercises or real-world incidents. Users may enter data from a finalized After-Action Report/Improvement Plan, track the progress of corrective action implementation, and analyze and report on trends in improvement plans.
* **Critical Business Functions** – The critical activities performed by organizations, especially after a disruption of normal activities. There are three (3) categories of critical business functions: National Critical business functions, Primary Mission Critical business functions, and Mission Critical business functions.
* **Delegation of Authority** – The identification, by position, of the authorities making policy determinations and decisions at headquarters, field levels, and all other organizational locations. Generally, pre-determined delegations of authority take effect after the disruption of the normal channels of direction and they lapse with the reestablishment of these channels.
* **Devolution** – The capability to transfer statutory authority and responsibility for critical business functions from an agency’s primary operating staff and facilities to other agency employees and facilities, and to sustain that operational capability for an extended period.
* **Emergency Management Plan** – A program that implements the mission, vision, strategic goals and objectives as well as the management framework of the organization. It includes three (3) main areas; an Emergency Response Plan that focuses on people’s safety; and the Business Continuity Plan(s), which address the performance of how the critical business functions will continue during a disruptive event; and a Disaster Recovery Plan that ensures the maintenance and recovery of the IT Infrastructure.
* **Emergency Response Plan (ERP)** – A guide designed to ensure the consideration of the health and safety of Company personnel, contractors, and visitors if an emergency occurs at work. It provides a brief overview of emergency procedures, evacuation, and key emergency contacts. It also establishes the roles, responsibilities, and command structure used during an emergency for the agency. A copy of the ERP is on the Company Intranet.
* **Essential staff members** – Those personnel, both senior and core, who provide the leadership advice, recommendations, and functional support necessary to continue essential operations.
* **Facilities** – The locations where an organization’s leadership and staff members operate. Leadership and staff members may be co-located in one (1) facility or dispersed across many locations and connected by communications systems. Facilities must be able to provide staff members with survivable protection and must enable continued and endurable operations.
* **Interoperable Communications** – The communications that provide the capability to perform critical business functions, in conjunction with other organizations/entities, under all conditions.
* **Leadership** –Senior decision makers.
* **Management Services Team** - This team; in conjunction with advisements from the command structure outlined in the ERP, informs the agency as a whole of current safety issues and status general in regard to an incident that could impact business and personnel wellbeing. They provide location access and associated resources as well as overarching communication needs to the agency.
* **Maximum Tolerable Downtime (MTD)** - How long the critical business function can be unavailable or not performed. Considerations include expected customer service levels, law and regulations, and political impact.
* **Memorandum of Agreement (MOA)/Memorandum of Understanding (MOU)** – The written agreement between departments/agencies that require specific goods or services to be furnished or tasks to be accomplished by one (1) organization in support of the other.
* **Mission Critical Business Functions** –The limited set of agency-level government functions that require continuance throughout or resumed rapidly after, a disruption of normal activities.
* **Orders of Succession** – The order in which there are provisions for the assumption by individuals of the organization’s senior leadership positions during an emergency in the event that any of those officials are unavailable to execute their legal duties.
* **Organization Head** – The highest-ranking official of the primary occupant organization, or a selected successor or designee by that official.
* **Primary Operating Facility** – The site of an organization’s normal, day-to-day operations, which is the location where the employees usually report for work.
* **Reconstitution** – The process by which surviving and/or replacement organization personnel resume normal operations from the original or replacement primary operating facility.
* **Recovery Point Objective (RPO)** - The point-in-time to which work (commonly in the form of data) should be restored following a business continuity event that interrupts the business, e.g. Data backed up every night indicates a one (1) day Restore Point Objective.
* **Recovery Team** – A division specific team responsible for maintaining the recovery procedures, as well as coordinating the recovery of the division’s business functions and processes during an event.
* **Recovery Time Objective (RTO)** - Identifying the time by which mission critical IT dependencies must be recovered to meet the Maximum Tolerable Downtime (MTD) for the business function
* **Risk Analysis** – The process of identifying and evaluating risks.
* **Risk Assessment** – The identification and assessment of hazards.
* **Risk Management** – The process of identifying, controlling, and minimizing the impact of events whose consequences are or may be unknown, or events that are fraught with uncertainty.
* **Salvage Team** – The objective of a team that saves vital records, equipment, function specific supplies, and manuals needed for recovery from a vacated location. The enactment of this occurs after Building Services confirms that the location is safe for occupation.
* **Telecommute** – The ability to work at a location other than the official duty station to perform work or emergency duties. This may include, but is not limited to, using portable computers, personal computers, high-speed telecommunications links, and mobile communications devices.
* **Testing, Training, and Exercises (TT&E)** – The use of measures to ensure that an agency’s Continuity Plan is capable of supporting the continued execution of the agency’s critical business functions throughout the duration of a continuity situation.
* **Virtual Offices** – An environment where employees are not in a co-location and rely exclusively on information technologies to interact and conduct their work across distance from multiple geographic locations.
* **Vital Records** – This term pertains to the electronic and hardcopy documents, references, and records that are necessary to support critical business functions during a continuity situation. The two (2) basic categories of vital records are (1) emergency operating records and (2) rights and interests records.
1. **Acronyms**

|  |  |
| --- | --- |
| AAR | After Action Report |
| BIA | Business Impact Analysis |
| BPA | Business Process Analysis |
| CGC | Continuity Guidance Circular |
| RT & ES  | Recovery Team & Essential Staff |
| IT | Information Technology |
| MEF | Mission Essential Function |
| MOA | Memorandum of Agreement |
| MOU | Memorandum of Understanding |
| MTD | Maximum Tolerable Downtime |
| RAP | Remedial Action Program |
| RPO | Recovery Point Objective |
| RTO | Recovery Time Objective |
| STTEF | State, Territorial, and Tribal Essential Function |
| TT&E | Test, Training, and Exercise |

1. **Directions to Remote Locations**
2.
3. **BCP Scenarios**
4. **Potential causes of interruptions and things to rehearse against**
5. **Rehearsing Lack of Access**
6. power failure
7. road closure
8. fire
9. flood
10. bomb
11. water outage
12. gas leak
13. bomb alert
14. structural damage
15. area evacuation
16. **Rehearsing Lack of People**
17. contagious illness
18. strike
19. transport outage
20. building closure (see ‘lack of access’)
21. using recovery location
22. **Rehearsing Lack of Infrastructure**
23. power outage
24. gas outage
25. water outage
26. IT network outage
27. loss of IT files
28. technology connection outage
29. loss of data
30. system application outage
31. telecoms outage
32. flood
33. **Rehearsing Crisis Management Response**
34. Anything in any other list!
35. Threats: e.g., bomb, cyber-attack, blackmail, data theft or loss, etc.