	Guideline: ITS Contingency Plan Management Procedure	
	Department Responsible: SW-ITS-Administration	**Date Approved:** 06/09/2021
	Effective Date: 06/09/2021	**Next Review Date:** 06/09/2022

INTENDED AUDIENCE:
Entire workforce

PROCEDURE:
In accordance with the standards set forth under federal and state statutory requirements (hereafter referred to as regulatory requirements), Cone Health is committed to ensuring the confidentiality, integrity, and availability of all protected health information (PHI/ePHI), confidential, and sensitive data (hereafter referred to as covered information) it creates, receives, maintains, and/or transmits. and sensitive data (hereafter referred to as covered information) it creates, receives, maintains, and/or transmits.

The purpose of this procedure is to define roles, responsibilities, and processes associated with Cone Health's contingency planning program.

Scope and Goals:
The scope of Cone Health's contingency plan program is to ensure business operations continues with minimal or no disruption during a localized or catastrophic disaster. Contingency management is combined planning efforts for the business continuity plan (BCP) and disaster recovery plan (DRP). Goals are as follows:

- Assign responsibilities for the management and maintenance of the contingency planning program.
- Plan to ensure the safety of the workforce, clients, and customers.
- Base plans on identifying events (or sequence of events) that can cause interruptions to critical business processes (e.g., equipment failure, human errors, theft, fire, natural disasters, and acts of terrorism).
- Minimize the loss of patient/client/customer and public confidence.
- Expeditious recovery of data with no loss or degradation to integrity.
- Facilitate the prompt resumption of services.
- Maintain security of covered information.

Responsibilities:
Emergency Management Director:
This role coordinates the contingency planning effort and moves the planning through all phases to completion and testing. The Emergency Management director is responsible for creating a Systemwide Emergency Management Committee comprised of representatives from senior management, functional areas and departments that are critical to the organization.

The Emergency Management director (with support from the Systemwide Emergency Management Committee) responsibilities include:

- Revisions, implementation, workforce education, interpretation and enforcement of this procedure.
- Ensure that the information security aspects of contingency plans are
  - Based on identifying events (or sequence of events) that can cause interruptions to the organization's critical business processes (e.g., equipment failure, human errors, theft, fire, natural disasters, acts of terrorism)
  - Followed by a risk assessment to determine the probability and impact of such interruptions, in terms of time, damage scale and recovery period (See Information Security Risk Management for full process)
  - Based on the results of the risk assessment, a contingency strategy will be developed to identify the overall approach to continuity
  - Once this strategy has been created, endorsement is provided by management, and a plan will be created using the guidance outlined in this document.
- Perform business impact analyses to evaluate the consequences of disasters, security failures, loss of service, service availability, safety and financial impact, recovery time priorities, etc.
- Create, maintain and monitor the effectiveness of the program.
- Create and maintain a Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP).
- Conduct periodic mock exercises and tabletop reviews at least twice a year with appropriate personnel to ensure that everyone understands what their responsibilities are in the event that all or part of the plan needs to be implemented. The Emergency Management Director will ensure the exercises are diverse and take into consideration all types of disasters/disruptions.
- Determine any needed changes to the program, report them to management, and assist departmental implementation.
- Review, evaluate, and change the plans as necessary to accommodate comments and recommendations provided by critical departments.
- Perform annual testing of the BCP and DRP and report the results to management.
- Establish and update relocation/alternate operating location plans and maintain the necessary supplies for emergencies.
- Perform BCP and DRP training with departments to ensure that all workforce members understand their individual obligations.
- Ensure the contingency planning framework addresses a specific, minimal set of information security requirements (see process outlined in this document below).
- Ensure the business continuity and disaster recovery plans are distributed to key contingency personnel or that they are provided access to the plan electronically.

Systemwide Emergency Management Committee:

In addition to assisting the Emergency Management director, the Systemwide Emergency Management Committee will assist with the design, development, and ongoing maintenance of a formal contingency planning program. The Systemwide Emergency Management Committee will work with the Information and Technology Services (ITS) department to ensure appropriate assets and resources are available to ITS for the disaster recovery program. The Systemwide Emergency Management Committee will also work with the Security Incident Response Team (SIRT) and participate in all relevant incident response testing and exercises to remain in a prepared state to respond to any incidents that affect the availability of the organization.

Chief Information Security Officer (CISO):

The CISO will be a member of the Systemwide Emergency Management Committee and is responsible for ensuring the continuity of security functions during a time of crisis. Security functions include physical and logical security of covered information, information technology assets, etc., and include the physical protection of workforce personnel, patients, clients/customers, etc. The CISO will work with the Emergency Management director to perform an annual business continuity and disaster recovery risk assessment that considers the following:

- Identify business processes and their impact on information security.
- Identify, quantify, and prioritize risks against key business objectives, assets, resources, etc.
- Identify critical resources, impact of disruptions against these resources, and allowable outage times and recovery priorities, as well as the need to update the BCP and DRP based on the risk assessment results.

Information and Technology Services (ITS):

ITS Management is responsible for:

- Participation on the Systemwide Emergency Management Committee.
- Creating and maintaining a disaster recovery plan that ensures the continuity of ITS operations during a time of crisis. The disaster recovery plan will address:
    - A formal definition of the level of backup required for each system, including how each system will be restored, the scope of data to be backed up, frequency of backups, and duration of retention based on relevant internal and external business dependencies, as well as contractual, legal, regulatory, and business requirements.
    - Appropriate activities to be performed to maintain ITS operations for specific disaster scenarios (i.e., natural, environmental, technology, etc.).
    - Required capacity (e.g., information processing, telecommunications, and environmental support is available during contingency operations) and identification of critical processes/functions.
    - Recovery point objective (RPO) and recovery time objective (RTO) for all business-critical systems, based on pre-defined business requirements.
    - Identification of roles and responsibilities and documentation of contact information.
    - Establishing alternate operating locations to prepare for and protect against catastrophic disasters that could occur that require the relocation of operations. These locations must be a sufficient distance away from the primary facility that they would not be affected by the same event. The security controls in place must be configured with measures equivalent to the primary site. For any third-party services used, the agreements that are established must allow for the resumption of information systems and the operation of critical business functions within the defined RTOs and RPOs.
    - Alternative internet service providers should an outage of a provider's service occur.
    - Alternate communication lines that are sufficiently separated from the primary service provider in the event the phone system goes down or commercial telecommunications is unavailable.
    - Emergency power (i.e., UPS and diesel generators) for information systems.
    - Succession planning for each role in the event someone is not available to fulfill their responsibilities during a crisis.

- Recovery and restoration of business operations and establishing availability of information in the time frame required by business objectives and without deterioration of security measures.
- Maintaining current data backups for all critical systems.
- Performing periodic tests of the disaster recovery plan to ensure everyone involved understands their responsibilities and that the plan is still current.
- Oversee data backup and offsite storage of backup media.
- Periodically restore data from backups to ensure that the process works and that the data is not corrupted.
- Ensuring that appropriate ITS personnel maintain an offsite copy of the disaster recovery plan, or have access to the plan that is stored at an offsite location, or is electronically accessible (should be independent of the organization's network as it may not be available during a disaster scenario).

Management:

Management will ensure the following in support of the contingency planning program:

- Allocating sufficient resources and knowledgeable personnel to develop the BCP and DRP.
- Setting policy by determining how the institution will manage and control identified risks.
- Reviewing BCP and DRP test results.
- Reviewing and approving the BCP and DRP on an annual basis.
- Ensuring the BCP and DRP are kept up-to-date and appropriate workforce members are trained and aware of their role in its implementation.

System/Application Owners:

System/application owners will work with the Systemwide Emergency Management Committee and ITS to ensure that their business recovery and continuation needs are met. System/application owners will be responsible for participating in tests, exercises, etc., when it is appropriate.

Business Units:

Business units are responsible for, but not limited to, the following:

- Creating their own unique business continuity plans for how they will respond and continue business in the event of disasters or disruptions that are unique to the unit. Examples of this could be loss of technology services, relocation due to facility damage, emergency staffing due to pandemic situations, environmental threats (i.e., tornado, earthquake, ice storm, etc.), fire, bomb threats, terrorist activity, etc.
- Annually reviewing business continuity plans for accuracy and familiarity.

Vendors:

Vendors who maintain systems/applications on behalf of Cone Health will establish their own formal BCP and DRP. The plans are required to be composed in a way that complies with the requirements defined in this procedure. Business continuity and disaster recovery requirements will be addressed in service level agreements or similar vendor contracts.

Defining the Contingency Plan Strategy:
The contingency plan strategy represents a critical aspect of contingency planning and is derived from the information collected during the business impact analysis (BIA) process. The following components must be considered when defining the contingency plan strategy and developing the related plans:

- Personnel (who owns the business continuity plan[s] and who needs to be involved)
- Communication (internal and external)
- Conditions to activate the business continuity plan as well as escalation plans
- Networking equipment and network services
- Technology issues (i.e., disaster recovery plan)
- Facilities (e.g., security, relocation, safety, emergency power and communications)
- Critical business processes and systems (e.g., RPO, RTO)
- Manual operations (i.e., what if technology resources are not available?)
- Resumption procedures which describe the actions to be taken to return to normal business operations
- Succession planning for each role in the event someone is not available to fulfill their responsibilities during a crisis

When developing the contingency plan strategy, consideration will be given to both short-term and long-term goals and objectives.

Short-term goals and objectives include, but are not limited to:

- Critical personnel, facilities, computer systems, operations, and equipment
- Priorities for processing, recovery, and mitigation
- Maximum downtime before recovery of operations
- Minimum resources required for recovery

Long-term goals and objectives include, but are not limited to:

- Management's enterprise-wide strategic plan
- Coordination of personnel and activities
- Budgetary considerations
- Supervision of third-party resources

System Backups:
System backups (i.e., data and software) are a critical component to Cone Health systems. Backups are used for a variety of functions including a required system restore, disaster recovery, historical data, and other contingency planning functions. All backup data at Cone Health adheres to the documented data at rest and data in transit encryption standards which is 256 AES. To ensure backups follow good security and availability practices, Cone Health abides by the following requirements:

- Daily backups are retained for 14 days. One backup from each of the three most recent months is also retained.
- A second copy of each backup is stored in a cloud provider storage account.
- Backups are completed before moving servers or hard drives to a new location.
- All backup data is transported and stored in an encrypted format. This applies to both electronic and physical media (i.e., backup tapes).

- Backup and recovery processes are validated periodically.
- An inventory for all backup data, including content and current location, will be maintained.
- The use of automated tools must be used to track all backups, both physical (backup tapes) and logical. At a minimum, tracking information will include a name, date, time, and action taken.
- Three generations of backups are stored off-site.
- For server migration that includes systems that contain PHI or other covered information, Cone Health will ensure a current, retrievable copy of the information is available before the migration occurs.
- Backup information is verified to ensure its accuracy using cyclic redundancy check (CRC) as it is being written to media, and as part of a continuous background scan to identify corruption and inconsistency in order to ensure the availability of the data.

Documentation Retention:
Retain all documentation associated with exercises, tests, etc., and previous versions of business continuity/disaster recovery plans for a minimum of 6 years.

Exception Management:
Exceptions to this procedure will be evaluated in accordance with Cone Health's Information Security Exception Management procedure.

Applicability:
All employees, volunteers, trainees, consultants, contractors, and other persons (i.e., workforce) whose conduct, in the performance of work for Cone Health, is under the direct control of Cone Health, whether or not they are compensated by Cone Health.

Compliance:
Workforce members are required to comply with all information security policies/procedures as a condition of employment/contract with Cone Health. Workforce members who fail to abide by requirements outlined in information security policies/procedures are subject to disciplinary action up to and including termination of employment/contract.