Liberty Healthcare Corporation and Affiliates (Liberty) Standard Operating Policies

Title:	**ISF 8.0 – Business Continuity Plan Policy**	**Effective Date:**	**12/28/2020**
Author:	**Haroon Ahmad**	**Last Review Date:**	**12/22/2021**
Location:	**All Locations**	**Last Revision Date:**	**12/22/2021**
Functional Area:	**All Areas**		

CONTENTS

8.0 BUSINESS CONTINUITY PLAN POLICY

8.1 PURPOSE

This policy is defined to provide guidance to all Liberty Healthcare Corporation and its affiliates (Liberty) programs and departments for the development and maintenance of requirements for a business continuity plan. These plans are document the critical aspects of a specific program or department and provide an understanding of any associated risks. A properly developed plan will provide guidance to program directors, executives, Technology Solutions, and all employees on their duties to assist in the prevention of potential continuity issue as well the prompt recovery of any affected business processes.

8.2 SCOPE

This policy applies to all portions of Liberty Healthcare Corporation and its affiliates. This includes all programs, contracts, facility locations, departments, and critical business operations.

8.3 POLICY

All Liberty programs and contracts are required to maintain a business continuity plan.

The Liberty Information Security Officer (ISO) is required to provide assistance and oversight during the development and maintenance of all business continuity plans for any specific program or contract, and to approve all documented plans.

The Liberty ISO must work with program directors and other appropriate personnel to ensure a given business continuity plan addresses all critical aspects of the programs business operations. Any additional requirements, either regulatory or contractual, should be considered and incorporated during the development of a given plan.

All business continuity plans must be reviewed, tested, and updated annually to ensure accuracy. These reviews are to ensure all documented capabilities, processes, and options remain valid and operate effectively. The ISO is required to oversee each annual review and ensure all relevant documentation, notes, meeting minutes, updates and mitigations are maintained. Plan documentation revisions must be identified and detailed as well.

All finalized business continuity plans must be approved by the program Executive Director and/or relevant business process owner, Liberty Healthcare's ISO, Liberty Healthcare's CIO/CTO, as well as applicable executive management.

8.3.1 Business Impact Analysis

In order to properly document and determine all components of a business and to understand all relevant risks to the business and operations, a Business Impact Analysis (BIA) should be performed, when applicable, prior to creating a program or contract specific business continuity plan.

The purpose of performing a Business Impact Analysis is to identify the critical assets, risks associated with the identified assets, and most importantly to identify potential risks that could impact to those assets and/or critical operations. An asset can be defined as any portion or resource of the business that is determined to be critical to the successful ongoing operations of the business. This includes but is not limited to, technology, devices, facilities, services, applications, employees, documents, business processes, etc.

The BIA should identify the assets and any relevant critical service level agreements (SLAs) pertaining to the contractual deliverables, as well as any other defined confidentiality and availability control requirements.

The BIA should classify all risks for each asset by identifying a risk impact level and potential risk likelihood. This risk classification provides an overview of all the critical aspects of the business operations in order to provide guidance during the creation of the business continuity plan.

8.3.2 Recovery Strategies & Process

In addition to performing the business impact analysis, specific planned or potential recovery strategies should be identified for each identified critical asset. These identified strategies and processes should detail alternative options for continuing an effected portion of the business, as well as detail the recovery process to return to a normal operation procedure.
The identified continuity procedures and recovery processes must also consider SLA requirements and deliverables defined by contracts, regulatory frameworks or critical business requirements. Additional Liberty defined SLAs or limitations – where appropriate – should be defined as well.

8.3.3 Plan Documentation Requirements

A completed Business Continuity Plan (BCP) document should include the following components (as well as any other program specific sections):

Emergency Planning Team – This team is the identified group of individuals required to identify and provide information pertaining to asset identification, business impact analysis, continuity procedures, and recovery process. This group, in conjunction with the Liberty Information Security Officer, are tasked with creating, maintaining, and reviewing the plan annually, as well as performing the plan test annually.

Business Location Information – This section requires detailing information for the physical facility location such as address, contacts, property management information, etc.

Emergency Response Team – This identified the group of individuals who will be responsible for initiating the Business Continuity Plan in the event of a potential or realized continuity event, or other severe degradation of a critical business process. This team will provide guidance and instruction to implement aspects of the plan to ensure business continuity and perform recovery operation procedures, as needed. This group is also responsible for notifying all appropriate stakeholders such

as employees, clients, Liberty executive management, etc., and keeping them informed throughout the life cycle of any continuity event.

Continuity and Recovery Procedure – This section of the plan documentation defines the process for utilizing the BCP in the event of a continuity event. This includes details surrounding employee safety, event assessment, notification requirements, implementation of contingency options, as well as the process for restoring to the normal operational procedures.

Alternate Facility – Provides all relevant information for alternate facilities (if appropriate) in the event a primary facility is no longer usable.

Data Backup and Restoration – This section provides details on critical business technology data backup processes and restoration procedures.

Technology Options – This section details technology services deemed foundational to the critical business processes, as determined by the business impact analysis, and provides information on contingency options or processes that are acceptable. Additional options and details can be provided in standalone sections of the plan for the most critical technologies or those that are specific to the business, program, or contract.

Business Operation Backup Processes – This section details the various critical business processes identified by the business impact analysis and provides specific information on available contingency processes to ensure continuity of business operations.

8.3.4 PLAN TESTING

All business continuity plans must be tested on an annual basis to verify all processes and defined contingency options continue to operate as designed. The Liberty Information Security Officer (or designee) is required to oversee the test in conjunction with program directors, IT, and any other applicable individuals, executive management, employees, contractors, and/or third parties.

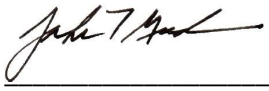
Wherever possible, all defined technical controls and contingency options should be tested to ensure expected operation levels while under a full and/or unexpected load.

Contingency business operation processes should also be tested to ensure operating effectiveness. These contingency options should be verified as usable with all resources reliably accessible in the event that a transition is needed.

Test results should be compiled and documented, detailing successes, failures, and issues, with any identified changes or updates documented in the business continuity plan. The Liberty Information Security Officer (or designee) is responsible for overseeing the documentation of the test results and subsequent changes.

APPROVALS

Haroon Ahmad – Information Security Officer



John T. Guda – CIO / CTO

REVISION HISTORY

Version	Date	Author	Summary of Changes
1.0	12/28/2020	Haroon Ahmad	Initial ISF release – refactor and update of previous security policies into distinct documents
2.0	12/22/2021	Haroon Ahmad	Annual review. No major changes