Liberty Healthcare Corporation and Affiliates (Liberty) Standard Operating Policies

Title:	**ISF 7.0 – Application Development 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

7.0 Application Development Policy 1

7.1 Purpose 1

7.2 Scope 1

7.3 Policy 1

7.3.1 Development Process 2

7.0 APPLICATION DEVELOPMENT POLICY

7.1 PURPOSE

This policy defines the processes in place at Liberty Healthcare Corporation and its affiliates (Liberty) to properly ensure company owned and managed applications are developed, updated, patched, and changed in an appropriate manner to consistently maintain the confidentiality, integrity, and availability of the data residing within the applications. These guidelines also set parameters for testing and approval requirements of initial development and changes before any applications or updates are used in a live production environment.

7.2 SCOPE

This policy applies to all applications licensed, owned, managed, and/or developed by Liberty to support Liberty business operations – whether they be used by an individual program, several programs, or are available across the Liberty enterprise. All such applications must be approved by Liberty Technology Solutions executive leadership, maintained as part of the Liberty Technology Solutions application inventory, and must adhere to all relevant and appropriate ISF policies and related procedures. Application may be licensed, internally developed, or developed utilizing third parties under appropriate contractual agreements approved and managed by Liberty Technology Solutions executive leadership. For avoidance of doubt, applications include those provided "as a service" (e.g., SaaS, IaaS, DaaS, etc.), as well as "as a service" utilities or add-ons to other Liberty applications. All applications, as defined above, are required to follow these guidelines to ensure uninterrupted services to Liberty employees, customers, and clients.

7.3 POLICY

The initial development and/or substantial change to an application must be approved by Technology Solutions executive management and will be guided by system and/or business requirements which provide the details that final product should incorporate. This includes all contractual and business required functions that affect the daily operation of the application or business processes. These requirements may also include requested user/customer functionality, deliverable changes, regulation updates, incorporated or mitigated defects, etc.

The initial development or changes must consider HIPAA compliance requirements as well as requirements set by other corporate policies, Liberty' Information Security Framework, Liberty's Development Security Standards Checklist, and applicable industry best practices, as appropriate.

All processes surrounding the initial application development and/or changes to Liberty managed applications must be tracked within Liberty's requirements documentation repository, feature and defect tracking repository, and/or appropriate ticketing system. Each development feature or change should be properly documented with details of each step of the development or change processes from the initial request through the final implementation.

A Liberty application will have an identified Business Application Owner (BAO) and Technology Solutions Application Owner (TAO), each of which will be documented within Liberty Application Inventory. The Technology Solutions application owner is responsible for approving and authorizing all development related actions, in collaboration with the Application Business Owner.

7.3.1 Development Process

7.3.1.1 Initial Design / Change Identification

All initial design requirements or changes should be identified and documented within the requirements tracking system to include appropriate details of the feature or change, including the source of the requirement.

7.3.1.2 Development Authorization

The BAO is responsible for defining the high-level business requirements and justification for development, procurement or significant additional investment in a new or existing application – working in conjunction with the TAO to inform cost, timeline, risk and benefit information. The TAO is responsible for arranging and managing the suppliers, developers and other resources that will deliver, manage and maintain the application – working in conjunction with the BAO. The TAO will lead the individuals involved in delivering, supporting sand maintaining the application – including defining design features and/or changes (e.g., scope) before development begins. Features and/or changes selected to be included within an initial or upcoming build or release should be documented within the appropriate support systems to ensure identification and tracking of changes. Alignment and/or changes to scope, timeline, cost or other material aspects of the application will documented within the tracking system and/or meeting minutes.

Any changes authorized for subsequent inclusion should be identified and documented in the requirements repository and /or defect and feature tracking system - as part of a new build version for appropriate tracking.

7.3.1.3 Development

All development activities and processes defined and managed by the application development management team, led by the TAO.

All development activities, whether performed in-house or in conjunction with third party developers, should include secure development practices whenever applicable, and reference Liberty's Development Security Standards documentation, and relevant industry standards and practices.

7.3.1.4 Development Testing

The purpose of development testing is to ensure that initial application development or change is operating within the parameters defined in the requirements documentation and relevant security best practices and standards, without introducing new unacceptable functional or technical defects.

Testing parameters should be identified, and all results documented within the testing management (if applicable) and defect tracking systems. These parameters can include specific feature testing requirements, defect testing requirements, as well as regression testing.

Once a design feature or change has been coded, the development team will utilize a testing environment to perform testing of the new change or feature. The development managers will perform the initial testing of the change or feature as well as review all aspects of the new application build version to verify no other defects have been introduced.

Additional testing may be performed by end users within the testing environment ensure all necessary features / changes have been adequately addressed and function appropriately to support Liberty business operations.

Any developed features or changes with insufficient or failed testing results will be identified as requiring rework within the defect tracking system, and a determination made to either rework the issue or defer the issue to a later version or release. To prevent delays, the initial feature or change in question can be removed from the current build version and added to another to provide sufficient time for more robust development to occur.

Once a change or group of changes in a build have successfully completed the testing phase, the changes can then be approved by TAO and BAO, the composite collection of features shall be determined to be a Release Candidate, that can be scheduled for deployment in support of Liberty business operations.

7.3.1.5 Release Candidate Review

Once the selected design, changes, and builds have completed the testing process, they will be compiled into the next version of the Release Candidate for the application. This review phase is to ensure all the logistical requirements of implementing the release are addressed. These are a few of the tasks required to be reviewed prior to implementation.

- Review all testing documentation to ensure completion
- Review timing and logistics of production implementation
- Define application downtime and provide notification to appropriate stakeholders.
- Ensure the availability of appropriate end-user education programs, release notes, and procedures documentation
- Identify roll back procedures

7.3.1.6 Production Implementation

To properly manage the process of implementing the Release Candidate into production, the TAO and designees will work all necessary parties to ensure a smooth application deployment process. The TAO will ensure a detailed Deployment Plan is defined and documented to ensure successful deployment, and the ability to rollback and changes if necessary. This plan will include step-by-step procedures, measures, timelines and checkpoints and communications plan that will be followed throughout the deployment process. The Deployment Plan will also identify critical decision points and rollback procedures – should this become necessary. The Deployment Plan will define a relevant point-of-no-return (PNR) - both during the deployment process, and subsequent to production activation – after which rollback and recovery will become infeasible.

7.3.1.7 Deployment Testing & Application Use

Subsequent to deployment of the new Release Candidate has into the production environment, and before making the system available to end-users, testing will be conducted to ensure the updated system is operating as expected. Liberty Technology Solutions personnel, along with select end-users (as appropriate). will perform a Smoke Test, which consists of testing key operational characteristics of the system to verify system operations, performance and security settings - updating as needed to provide a stable operating environment.

Once the Smoke Test has been successfully completed and documented (and no unacceptable defects or issues have been uncovered), the system will be made available to users.

Subsequent to activation of the new production application, the TAO and BAO will ensure that the system is closely monitored to ensure it is operating acceptably and as expected. Details of the deployment process and results of the Smoke Test should be documented within the tracking system.

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