

Title:	ISF 9.0 – Vendor Management 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

9.0	Vendor Management Policy	1
9.1	<i>Purpose</i>	1
9.1	<i>Scope.....</i>	1
9.2	<i>Policy.....</i>	1
9.2.1	Vendor Selection	2
9.2.2	Vendor Agreements	2
9.2.3	Vendor Risk Assessment Requirements	2
9.2.4	Vendor Risk Assessment Controls	2

9.0 **VENDOR MANAGEMENT POLICY**

9.1 **PURPOSE**

This policy is design to provide all of Liberty Healthcare Corporate and its affiliates (Liberty) with guidance on controls to consider while selecting and/or contracting a potential vendor or third party to work with Liberty, as well as to provide a set of controls to be reviewed to ensure any Liberty Confidential information (including any and all PHI data) that is managed, stored, or accessed, by the third party is handled and secured in a manner acceptable by Liberty Healthcare. With a review of relevant data security controls, Liberty is able maintain a high level of confidentiality and integrity of all confidential data and reduce the risk of a potential unauthorize disclosure of data.

9.1 **SCOPE**

This policy applies to all current and potential vendors across the Liberty Corporation with the ability to access, manage, store, or utilize Liberty Confidential Information, systems, and applications. The categorization of vendors or third parties deemed critical and to be reviewed in accordance with this policy should be determined by the Liberty Information Security Officer (ISO), in conjunction with Liberty Technology Solutions, legal and business operations leadership. Components of a vendor risk assessment may be added or removed to more accurately perform the review based on the scope of the work defined within a contract, work order or other similar agreement.

9.2 **POLICY**

The Liberty ISO is responsible for reviewing all in-scope vendors and third parties to understand the capabilities and potential risks created by working with non-Liberty entities.

Any vendor or third party that has access to Liberty Confidential Information in any manner – such as storing, managing, reviewing, creating, or transmission of the data – should be subjected to a vendor risk assessment. The vendor risk assessment process must be completed by the Liberty ISO (or designee).

The vendor risk assessment results should be made available to applicable stakeholders such as business process owners, program directors, executive management, and any other applicable parties to ensure identified risks are reviewed. All identified risks should be deemed acceptable by the applicable stakeholders and the ISO or determined to be a critical risk requiring the ISO (or designee) to work with the vendor or third party to mitigate the risk to an acceptable level.

9.2.1 VENDOR SELECTION

A vendor risk review should be performed during the vendor selection process to consider the third party's capabilities to ensure the confidentiality and integrity of any provided Liberty Confidential Information.

9.2.2 VENDOR AGREEMENTS

All vendor agreements and contracts should include wording detailing the third-party entity's responsibilities for ensuring confidentiality, integrity, and availability (when applicable) for any Liberty Confidential Information in scope. The agreements must also define the third party's HIPAA responsibilities.

All Liberty vendors or third parties with access to Liberty Confidential Information must enter into a Business Associates Agreement approved by Liberty legal.

When applicable, vendor agreements should detail specific information security requirements determined by Liberty to ensure proper protections surrounding any provided Liberty Confidential Information. These agreements should also include the ability for Liberty to perform an information security risk assessment of the vendor or third party (at a minimum, annually) to verify the continued acceptable use of appropriate information security controls pertaining to all Liberty Confidential Information.

9.2.3 VENDOR RISK ASSESSMENT REQUIREMENTS

All in-scope Liberty vendors and third parties (i.e., that have access to or manage Liberty Confidential Information) should receive a vendor risk assessment, at the discretion of the Liberty ISO, working conjunction with Liberty Legal and business operations executive leadership.

A vendor risk assessment must be performed at a minimum annually for any applicable vendors or third parties.

The vendor risk assessment will review all relevant business operations, IT controls, and other relevant departments related to the security and protection of any Liberty Confidential Information.

A vendor risk assessment report will be completed by the Liberty ISO (or designee) to provide all relevant stakeholders insight into the potential risks surrounding any provided Liberty Confidential information. These risks should be either be approved or identified as requiring mitigation by the entity under review.

All assessment records and documentation will be maintained by the Liberty ISO (or designee).

9.2.4 VENDOR RISK ASSESSMENT CONTROLS

The controls listed below are guideline of the potential controls that should be reviewed as applicable when completing a vendor information security risk assessment. These controls, as well as any others that may not be listed, can be used at the discretion of the Liberty ISO or other designated assessor.

Business Operations – Review of the business operations to gain a proper understanding of the data workflow to verify security is considered throughout the processes.

Human Resources – Review to include training requirements, background check processes, onboarding and termination procedures.

Information Security Policies and Procedures – Review vendor defined policies and procedures and requirements surrounding confidentiality, data integrity, availability of all data.

3rd Party Attestations or Certifications – valid reports may be utilized to complete or replace portions or all of the vendor risk assessment.

Risk Management – Review a vendor’s ability to manage potential risks to critical data.

Incident Management – Review a vendor’s ability to manage incidents involving critical data.

Business Continuity & Disaster Recovery – Review to ensure a vendor’s ability to ensure continuity of operations in the event of a business interruption or disaster while maintaining confidentiality of data.

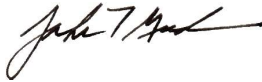
Secure Development – Review to ensure vendors follow best practices regarding secure coding software development processes, as appropriate.

Systems Monitoring – Review a vendor’s capability to monitor all systems to ensure controls are operating effectively as well as to identify any potential vulnerabilities.

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