Liberty Healthcare Corporation
THE FREEDOM TO SUCCEED™

Liberty Healthcare Corporation and Affiliates (Liberty) Standard Operating Policies

Title:	**ISF 11.0 – System Security 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

11.0 SYSTEM SECURITY POLICY

11.1 PURPOSE

The purpose of this policy is to provide a baseline of technical control requirements and guidelines for all Liberty Healthcare Corporation and its affiliates (Liberty) information systems. These requirements and guidelines are in place and designed to protect and maintain the confidentiality, integrity, and availability of all critical and sensitive data and systems including Liberty Confidential Information, employee information, business operations, intellectual property, trade secrets, technical and security controls, and any other sensitive information.

11.2 SCOPE

These identified controls, requirements, and guidelines are applicable to all Liberty information systems, all systems or devices that may store Liberty Confidential Information, and all devices that have or may have access to Liberty Confidential Information. This includes, but is not limited to, user workstations, servers, purchased application solutions, cloud environments, internally developed applications, mobile devices, removable media, or any other information system or device with access to any sensitive information created or managed by Liberty Healthcare.

11.3 POLICY

All endpoint devices - such as workstations and mobile devices – that maintain or have access to Liberty Confidential information must be managed by Liberty Technology Solutions and incorporate end-point management software configured to meet Liberty’s standards and requirements.

All endpoint devices are required to enforce password authentication for any users to access.

All endpoint devices are required to implement device encryption.

All endpoint workstations are required to lock the screen after a 15-minute period of inactivity after which a user must reenter their password to continue use.

All applications installed on any Liberty-provided endpoint devices must be reviewed and approved by Technology Solutions and Liberty's ISO. General users must not have the ability to install applications directly to any Liberty-provided endpoint devices.

All servers – premise or cloud-hosted - must implement device level encryption or data level encryption when applicable.

Any non-Liberty devices to be used in conjunction with any Liberty data and/or information systems must be pre-approved by Technology Solutions and configured to comply with all applicable Liberty security and technology standards prior to use.

The use of removable storage media is prohibited and must be disabled for all endpoint workstations and devices where practicable. Exceptions for use of removable storage require approval from Liberty's ISO and Technology Solutions executive leadership. If removable media is approved, appropriate asset tracking is required for each removable device within Liberty's asset management system is required. Any removable devices must be encrypted prior to use following the standards defined within the Data Management Policy.

Recording of calls, meetings, or video conferences is expressly prohibited for any applicable applications or services. Exceptions may be made by executive management to support contractually required recording, and the prerecording of training materials. All recorded content must be reviewed to ensure no critical information is available prior to distribution or further use.

11.3.1 Network Security

All network devices, including but not limited to firewalls, switches, and routers, must be managed by Liberty Technology Solutions and secured, require password authentication for authorized users to access.

Logging should be enabled on all devices to ensure all security changes are appropriately documented. When possible, notification of security changes should be enabled.

Firewalls must include an initial deny all rule for incoming and outgoing connections to prevent any unauthorized connections not required for essential business operations.

All wireless connections must require encrypted password authentication. Liberty wireless network connections should be utilized for business purposes only.

As appropriate, a separate wireless guest network may be provided for authorized individuals. The guest network must be segmented separately from the business wireless network to prevent any potential unauthorized access to sensitive company information.

In the event that device will need to connect to the company network and is not Liberty managed (such as a visitor workstation), the device will need to be reviewed by Liberty Technology Solutions and/or Information Security to ensure safety. Antivirus, patches, updates, definitions, and any other security controls deemed applicable may be reviewed for compliance with current Liberty IT standards.

11.3.2 Internet & Email Security

Access to any known malicious sites should be disabled.

Access to any websites containing any illegal or adult content should be disabled.

Emails containing known malicious content should be blocked or quarantined.

11.3.3 Backups

All Liberty data should be appropriately backed up to ensure integrity and availability of information as defined by the standards set by Liberty Technology Solutions.

All backups must be encrypted following the standard company protocols.

All backups of Liberty data must also consider the retention requirements detailed within the Data Retention section of the Data Management Policy.

11.3.4 Antivirus

All Liberty information device and systems must utilize antivirus software to protect against potentially malicious intent.

The antivirus software must not allow users to disable the protection without proper approval and oversight by Liberty Technology Solutions.

The antivirus software must update to the latest security definitions at least on a weekly basis.

The antivirus software should be configured to perform a full system scan at least on a weekly basis.

11.3.5 Patch Management

All Liberty information systems should be patched and updated with the latest security and critical updates at least on a monthly basis, when applicable, and as defined by Liberty Technology Solutions. Any applicable devices should be supported and licensed by the supplier to ensure appropriate patches and updates are provided

If possible, and where appropriate, patches and updates should be tested in a separate test environment prior to implementation on any production systems.

Any zero-day or emergency patches may be installed immediately, however should be monitored post implementation to ensure proper function.

11.3.6 Logging and Monitoring

Liberty Technology Solutions services will implement logging and monitoring capabilities of systems or networks, where applicable, to provide for the ability to review and monitor the appropriate use of information systems.

Systems and networks should be monitored with notifications of key or critical events to appropriate administrators of any unknown misuse or unauthorized accesses. These notifications may include but are not limited to the follow: change in configurations, change in security controls, access of critical data, non-compliance, failed access attempts, and any other deemed to be appropriate.

Internal and external vulnerability scanning should be performed on any applicable systems or networks on at least a quarterly basis to identify any existing or new vulnerabilities. Identified vulnerabilities should be mitigated and addressed appropriately.

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. Added inactivity lock requirement