

Title:	ISF 4.0 – Access 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

4.0	Access Management Policy	1
4.1	<i>Purpose.....</i>	1
4.2	<i>Scope.....</i>	1
4.3	<i>Policy.....</i>	1
4.3.1	Account Authorization.....	1
4.3.2	Account Requirements.....	2
4.3.3	VPN Remote Access Requirements	3
4.3.4	Mobile Phones.....	3
4.3.5	User Access Reviews.....	3

4.0 ACCESS MANAGEMENT POLICY

4.1 **PURPOSE**

Liberty Healthcare Corporation, and its affiliates (Liberty), has established the following policy to define appropriate requirements and guidelines for managing access and authorization to information systems, applications, and services. This policy will cover access parameters as well as all the stages in the life cycle of user access from initial authorization to termination.

4.2 **SCOPE**

This policy applies to all Liberty managed information services, devices, and applications. This includes but is not limited to the following examples: Active Directory, email, cloud services, ticketing systems, off the shelf applications or services, Liberty proprietary applications, workstations, servers, etc.

4.3 **POLICY**

4.3.1 **ACCOUNT AUTHORIZATION**

4.3.1.1 **Account Creation / Change**

The creation or changing of access levels of a user account for any Liberty information system must receive prior authorization from appropriate management – typically the program executive director or above (or designee), or department director or above (or designee) - who must approve requested changes. All requested changes must be detailed, with the appropriate approvals, within the Liberty ticketing system.

To receive a new account, all newly Liberty hired employees, subcontractors, and third parties must review and acknowledge the requirements defined within ISF 3.0 Acceptable Use Policy prior to initial access to information systems.

4.3.1.2 Account Termination

Termination of any user account requires prior authorization from appropriate management. The user's supervisor, system owner, or IT may backup or forward any user account data as needed to support Liberty business operations.

All accounts associated with a terminated employee must be disabled, deleted, or redirected within 24 hours of the official termination date to limit unauthorized data access or data loss.

All terminations of employees or staff, including the details of subsequent data handling, must be detailed, with all appropriate approvals, within the Liberty ticketing system.

4.3.2 ACCOUNT REQUIREMENTS

4.3.2.1 Standard Username Structure

The standard naming convention for user account names is *firstname.lastname*. For example, the default structure for Liberty email addresses is: *firstname.lastname@libertyhealth.com*.

This structure should be used for any application, service, or device whenever possible. Exceptions may be made by IT to address system or application limitations or additional identification requirements. Additional options, such as the use of middle initials, suffix, and numbers, may be used to avoid any potential duplicates.

4.3.2.2 User Group Management

User accounts' permissions within any Liberty application, system, or service should be defined by User Roles, Groups, and/or Security Profiles. These roles, groups, and security profiles are compiled and managed by Liberty IT to meet business and/or program specific needs.

General users are defined as users that do not retain the ability to perform any system or devices changes and are not able to perform any new software installations without prior approval.

Privileged users are system administrators, or other roles with elevated security privileges. These approved roles and individuals have the ability to access critical information systems, perform system changes, and install applications based on their individually defined job roles.

4.3.2.3 Password Requirements

All user accounts for any system, service, or application managed by Liberty Healthcare, are required to follow and maintain secure passwords that abide by the following rules:

- Passwords are required to have a minimum of 8 characters.
- Passwords are required to have complexity requirements enabled, requiring passwords to contain 3 of the following character types:
 - o Lowercase letter
 - o Uppercase letter
 - o Number (0-9)
 - o Non-alphanumeric special characters or symbols
- Passwords are required to have a minimum age of 1 day (when possible).
- Passwords are required to have a maximum age of 90 days (when possible).

- Passwords are required to not be identical to the previous 12 remembered passwords used for the given account (when possible).
- Passwords should not contain any common words, phrases, or passwords.
- Passwords should not contain any personal information such names, family names, address, birthday, phone numbers, etc.
- Any temporary passwords issued must be forced to be changed during the initial logon.

4.3.2.4 Account Lockout Requirements

All user accounts for any system, service, or application managed by Liberty Healthcare, are required to abide by the following account lockout limitations:

- 5 invalid password attempts will result in a locked user account
- Locked accounts are required to remain locked for a period of not less than 30 minutes following 5 invalid password attempts. Users may contact Liberty Technology Solutions for further assistance.

4.3.3 VPN REMOTE ACCESS REQUIREMENTS

To obtain access to a Liberty VPN (Virtual Private Network) for remotely accessing a Liberty secure environment, a request must be made following the appropriate requirements set in Account Authorization section above.

4.3.3.1 Restricted Devices

For any remote access via a VPN into the Liberty networks, all authorized users may only connect using a device approved by Liberty Technology Solutions.

4.3.3.2 Multifactor Authentication

MFA (Multifactor Authentication) is required for all VPN connections.

For the initial authentication method, all VPN users will be provided a username and password specific for the VPN service. This account is separate from the Liberty corporate domain account. The username format will follow the default structure previously described. The password must also abide by the password requirements previously defined.

A secondary authentication method is required for remote VPN access to Liberty applicable information systems. Liberty Technology Solutions will define the appropriate authentication process for each applicable system.

4.3.4 MOBILE PHONES

All mobile phones (iOS or Android) provided for company use by Liberty Technology Solutions services are required to follow an additional set of access controls.

- Passcodes are required to unlock the device
- The minimum passcode length must be no less than 4 numeric characters
- The maximum passcode age is 365 days.
- Passcodes are required to not be identical to the previous 5 remembered passcodes used for the given account.
- The mobile phone screen must lock after 5 minutes of in activity.
- The mobile phone must be wiped after 10 failed passcode attempts.

4.3.5 USER ACCESS REVIEWS

All employee accesses, permissions, accounts, and approvals for any Liberty system, application, device, and/or service, must be reviewed annually for accuracy and approved by an employee's

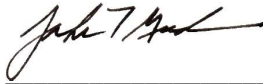
manager, data owner, or system owner, with the final approval by the program director (when necessary) or designated departmental manager.

Any changes made to a user's access or account's permission must be appropriately requested and documented through the Liberty ticketing system. Additionally, any meeting minutes, notes, and final approvals surrounding the review process must be documented and retained within the ticketing system for auditing requirements. The documentation must be made available, upon request, to the Information Security Officer for review.

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. Updated training requirements.