

<b>Title:</b>	<b>ISF 10.0 – Physical Security Policy</b>	<b>Effective Date:</b>	<b>12/28/2020</b>
<b>Author:</b>	<b>Haroon Ahmad</b>	<b>Last Review Date:</b>	<b>12/22/2021</b>
<b>Location:</b>	<b>All Locations</b>	<b>Last Revision Date:</b>	<b>12/22/2021</b>
<b>Functional Area:</b>	<b>All Areas</b>		

## CONTENTS

<b>10.0 Physical Security Policy .....</b>	<b>1</b>
10.1 Purpose .....	1
10.2 Scope.....	1
10.3 Policy.....	1
10.3.1 Facility Access & Badging .....	2
10.3.2 Secure Areas.....	2
10.3.3 Confidentiality .....	2
10.3.4 Visitors.....	2
10.3.5 Safety.....	3
10.4 Enforcement .....	3

## **10.0 PHYSICAL SECURITY POLICY**

### **10.1 PURPOSE**

The purpose of this policy is to establish guidelines and provide a baseline of physical controls related to accessing Liberty Healthcare Corporation, and its affiliates (Liberty) facilities, as well as ensuring controls for all critical assets. This document also defines requirements for granting, removing, and monitoring access.

### **10.2 SCOPE**

This policy applies to all Liberty facilities where Liberty Confidential Information is created, stored, managed or accessed.

### **10.3 POLICY**

All Liberty employees and staff are responsible for maintaining the security of any Liberty facility.

Access to Liberty facilities is restricted to only allow employees, authorized visitors, and any other expected and approved individuals.

Access to any physical media containing confidential information or access to physical information devices storing, maintain, or accessing confidential information, must be restricted to authorized individuals.

In addition to the baseline policies defined within this document, individual programs may require additional specific physical security policies and procedures as required by contracts, regulations, or to address specific business needs.

### **10.3.1 FACILITY ACCESS & BADGING**

All employees and authorized individuals should be assigned company badges that should be worn at all times at any Liberty facilities, when deemed to be appropriate.

When applicable, employees and authorized individuals may be assigned access badges/electronic keys to allow entry into the facility. Access badges should maintain appropriate but limited accessible hours to the facility.

All Liberty facilities and locations should maintain security monitoring alarm systems and notification processes for controlling and tracking access.

Employees are required to maintain the security surrounding any access badges, keys, codes, etc. for all Liberty facilities, locations, cabinets, closets, rooms, etc.

All employees are required to notify their supervisors, management, security officer, IT, or any other appropriate individuals in the event their access identification or access badge or other access control mechanism is lost, stolen or otherwise compromised.

Employees or other authorized individuals must ensure that unidentified/unauthorized persons are not allowed to enter any Liberty facilities or secure areas, including the exercise of caution to avoid "piggybacking" (following an authorized individual into a Liberty facility or secure area).

Access badges or other control devices must be surrendered to appropriate management upon any employee terminations. Additionally, badge access for any terminated employee should be disabled immediately.

### **10.3.2 SECURE AREAS**

Additional security measures must be maintained for secure areas or any location where confidential information is stored, as well as any other facility areas deemed critical to business operations. These areas include, but are not limited to, server rooms, communication rooms, print and mail rooms, electrical power controls, networking closets, executive offices, as well as any other identified unique locations.

Security controls must be maintained for any critical systems, data, or confidential information that is located in a more open location where the potential risk of unauthorized access is greater. These components should be controlled at all times by constant visibility by an authorized individual, or by localized security controls such as key or combination locks.

A list of all individuals authorized to access specific secure areas must be maintained. This list of authorized individuals must be reviewed and updated at a minimum annually to ensure all individuals authorized are valid.

Video surveillance is required for locations with access to or storage of Liberty Confidential information, to provide additional security monitoring, deterrence, and assurance, and for documenting access for HIPAA compliance, as applicable.

### **10.3.3 CONFIDENTIALITY**

All employees are required to maintain security surrounding all Liberty Confidential data and any other critical systems or sensitive information.

It is the responsibility of all Liberty employees to ensure no confidential information, or systems which access confidential information, are left unattended or unlocked.

No unauthorized use of recording devices, audio or video is allowed to be used within any Liberty facilities.

### **10.3.4 VISITORS**

All visitors accessing Liberty facilities must provide acceptable government issued photo identification prior to entering the location.

A record log of all visitors and non-employee individuals must be maintained. This information should include name, date, purpose of visit, verification of ID, and any other information that may be deemed applicable.

Visitors should be directed to access and exit the facility through one designated facility entrance.

Visitors may be required to review, complete, and sign a non-disclosure agreement as deemed applicable.

Visitors must not be left unattended in any part of the facility and must be escorted at all times, as deemed appropriate.

Visitors may be subject to searches of their bags, luggage as they enter or exit the facility.

In the event of an emergency, a visitor's escort is responsible for ensuring the safety of their visitor.

### **10.3.5 SAFETY**

All Liberty facilities and locations are required to maintain evacuation plans that are up to date and valid.

All Liberty facilities and locations are required to ensure building safety measure are compliant with local, state, and federal regulations.

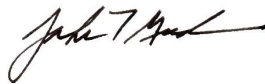
## **10.4 ENFORCEMENT**

Any employee found to be non-compliant and to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Refer to Liberty HIPAA SOP #3 – Complaints, Sanction, and Non-Retaliation for more information regarding the company's enforcement policies.

### **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 changes