TITLE: **INFORMATION SYSTEMS PASSWORD**

PURPOSE: To describe the requirements for creating passwords and utilizing other security features to protect against unauthorized access to Harris Health System's information systems.

POLICY STATEMENT:

Harris Health System will maintain access controls that require strong and unique account passwords for information systems. These access controls assist the Harris Health System in protecting information systems and resources from unauthorized access.

POLICY ELABORATION:

This policy applies to all Harris Health System Workforce members and Business Associates using or accessing Harris Health System information or information systems.

I. DEFINITIONS:

A. **CHIEF INFORMATION SECURITY OFFICER (CISO)**: An individual responsible for the management and supervision of the use of security measures to protect data and the conduct of personnel in relation to the protection of data as further defined in Harris Health Policy 3.11.801 Security Official Roles and Responsibilities.

B. **PRIVACY OFFICER:** An individual designated by Harris Health System to be responsible for the development and implementation of the privacy-related functions of Harris Health System as further defined in Harris Health Policy 3.11.101 Privacy Officer, Roles and Responsibilities.

C. **SYSTEM ADMINISTRATOR:** The individual responsible for the operations of maintaining a computer system. These operations include, but are not limited to:

1. User account creation/modification/termination;
2. System backups; and/or
3. System configuration changes.

These activities may be performed independent of, or in conjunction with,

Harris Health System's Information Security or Information Technology departments.

D. **VIOLATION:** An infraction of a HIPAA or other privacy or security policy, procedure, safeguard, or law that may or may not result in damage to Harris Health System or exposure of Harris Health System to liability, fines, or penalties.

E. **WORKFORCE:** Harris Health's Board of Managers, employees, medical staff, trainees, contractors, volunteers and vendors.

II. PASSWORDS:

A. The Information Security Department has developed the following password standards for Harris Health System:

1. Passwords must be changed every ninety (90) days.
2. Passwords may only be reused after four (4) different passwords have been previously used.
3. Where possible, passwords must contain three (3) of the following four (4) character types:

    a. Lower case alpha characters;
    b. Upper case alpha characters;
    c. Numbers; and
    d. Special characters (*e.g.*, !, $, #, % etc.), where allowed by the system.

4. Passwords must have a minimum of eight (8) characters.

B. After five (5) failed log in attempts, the system account will be locked, and the Workforce member must request a reset of the account through the Self Service Password Reset tool or by calling the Information Technology Service Desk.

C. Individuals with named user accounts shall not share passwords with anyone.

D. Passwords for named user accounts must be memorized and Workforce members should never document or record passwords with any corresponding account information or user names.

III. SCREEN LOCKING:

A. Workforce members who leave their computer workstation are required to manually lock their computers.

B. All computers, unless otherwise authorized, shall be configured to automatically invoke the screen saver after a period of inactivity. After five (5) minutes of inactivity, the screen will fade to black to shield the screen from plain view. After an additional five minutes of inactivity (ten (10)-minutes total) the screen saver will activate and will require the user to enter a password to unlock the computer. These controls will help protect computers from unauthorized access.

C. Screens can be locked manually by depressing the Crtl-Alt-Delete button and selecting "Lock This Computer" on the options screen.

IV. ENFORCEMENT AND EXCEPTIONS:

A. Any Workforce member found to have violated this policy may be subject to disciplinary action as outlined in the Harris Health Policy No. 3.11.104 Sanctions for Failure to Comply with Privacy and Information Security Policies.

B. Requests for exceptions to the Screen Locking procedures in this policy must be submitted in writing, with a business justification, to the CISO. The CISO and the Privacy Officer will evaluate the request for approval or disapproval. Requests for exceptions may be submitted at *informationsecurity@harrishealth.org*.

REFERENCES/BIBLIOGRAPHY:

Harris Health System Policy and Procedures 3.11.104 Sanctions for Failure to Comply with Privacy and Information Security Policies.

Harris Health System Policy and Procedures 3.11.800 Information Security Policy.

OFFICE OF PRIMARY RESPONSIBILITY:

Harris Health System Office of Corporate Compliance

REVIEW/REVISION HISTORY:

Record reviews and revisions below:

Effective Date	Version # (If Applicable)	Review or Revision Date (Indicate Reviewed or Revised)	Reviewed or Approved by: (If Board of Managers Approved, include Board Motion #)
04/20/2005	1.0	Approved 04/20/2005	President/CEO
	2.0	Revised/Approved 06/20/2006	HCHD Policy Review Committee
	3.0	Revised/Approved 05/13/2014	Operations Policy Committee
	4.0	Revised/Approved 07/08/2015	Operations Policy Committee