HEALTHQUEST

Title: Password Standard Policy	Type/Number: *HQ 5.9*
Effective Date: December 1st, 2015	Owner: *CISO, HQ IT*

For use at:

☒ HQ System, Inc (**ALL**)	☐ The Thompson House	☐ Northern Dutchess Hospital
☐ HQ Medical Practice	☐ Health Quest Urgent Care	☐ Putnam Hospital Center
☐ Health Quest Heart Center	☐ Health Quest Home Care	☐ Vassar Brother Medical Center
		☐ Other:

POLICY

Health Quest IT manages and is responsible for password creation and its management process. The Health-Quest Password Standard is defined by the requirements that need to be in place to effectively protect sensitive data and ensure full compliance with Health Quest's business requirements, regulatory requirements and industry standards.

Health-Quest IT Management will ensure and enforce the following are included in the Password Management requirements:

- Introduction/Authentication
- Access levels and privileges
- Creation and maintenance of long, strong, and unique passwords
- Protection of passwords
- Management and security of "Privilege Level" passwords
- Managing passwords including its reuse, forbidden dictionary of passwords, along with mandatory duration changes (90 days)
- Software applications
- Remote access
- Security Awareness and Training
- Network operating systems (OS)
- Enforcement

PROCEDURES

1.1 Access levels and passwords

The classifications of Health Quest's information assets determine the type of accounts and passwords required for access to information assets. The types of passwords include:

- Privileged level passwords for system administrators
- Production system level passwords for application developers and other administrators (e.g. database administrator)
- User level passwords for end users
- Password on accounts that are used for system to system interfaces. These are not used by users and are set by system administrators and approved by the CISO with mitigating controls. Because they are integral components of working systems, they are usually set to not expire

1.2 Creation of long, strong and unique passwords

It is very important to create long, strong and unique passwords that are hard to guess, periodically changes so that it can be misused by an unauthorized person and/or exploit by malicious attackers. The following two sub-sections describe the characteristics of weak and strong passwords.

1.2.1 Weak passwords

A weak password has the following characteristics:

- Contains less than eight characters
- Is a word that is found in the dictionary (English or foreign language) or easily referenced to work area and/or the end-user.
- A commonly used word associated with the account user. Examples include computer terms, commands and names of family members, pets, friends, co-workers, celebrities and fantasy characters
- Personal information such as birthdays, home addresses and phone numbers
- Word or number patterns such as 123123123, aaabbb, etc.

1.2.2 Strong passwords

A strong password must have the following characteristics:

- Contain at minimum 3 of the 4 of the character sets found on a standard keyboard: Upper Case letters, Lower Case letters, numbers and special characters
- Must be at least eight alphanumeric characters in length
- Does not contain a word found in the a dictionary, slang or dialect
- Not based on personal information such as family name, addresses, pets, children, etc.
- Not be based on your work environment including name of business or area of occupation, etc.
- Can be a passphrase for ease of remembering. An example is using a passphrase based on a song title such as “This May Be One Way To Remember”. The passphrase can be TmB1w2R or some other variations.
- Minimum password age. At most, passwords can only be changed by the user once a day—longer is preferred depending on the abilities of the application and the sensitivity of the data in the application
- Password history. Sufficient password history should be maintained such that a password, when it expires, cannot be reset or reused to the same password the user just had. This control works in conjunction with minimum password age to ensure it is effective reuse. A minimum of 5 passwords will be stored in history.

1.3 Protection of passwords

The confidentiality of passwords must be protected to prevent unauthorized access to Health Quest’s information assets. The following are guidelines which Health Quest personnel must adhere to ensure the confidentiality of their passwords:

- Passwords must not be inserted into email messages or any form of electronic communication except when they are first issued as notification to a manager
- Where SNMP is used, the standard defaults such as public, private and system must be redefined and different from the passwords used to log in interactively.
- A keyed hash must be used where available (e.g. SNMPv2) to protect the password
- Passwords must not be written down or stored on-line
- Health Quest account passwords must not be used for non-Health Quest accounts (e.g. online savings account, health benefits accounts, etc.)
- For Health Quest accounts, there must be unique password for each account
- For Health-Quest accounts password durations are not to exceed 90 days without the written compensating controls and the approval of the CISO
- All passwords must be confidential and not shared with anyone (e.g. administrative assistants, secretaries, co-workers, etc.) except as needed to distribute to new users.

1.4 Managing passwords

Management of passwords are different for each type of access levels:

- User passwords should expire every 90 days--
- For account holders who have system level privileges (granted through group memberships or programs), each account holder must ensure that the passwords for all their accounts are unique
- If there is any suspicion that an account has been compromised, the end user must immediately inform the CISO Office and change the password
- User accounts will be locked out after a maximum of 5 invalid login attempts within a 30 minute period.
- The Help Desk is responsible for resetting lost passwords, providing initial passwords. They must authenticate the end user prior to these actions.

1.5 Software applications

Application developers must ensure that all software applications have the following:

- Support authentication of individual users
- Not store passwords in clear text or in any easily reversible form. Using encryption/decryption features to protect the confidentiality of the passwords in storage and transmission for authentication
- Support TACACS+, RADIUS and/or X.509 with LDAP security retrieval, wherever possible

1.6 Remote access users

The password used for remote access must meet the long and strong password requirement.

1.7 Security Awareness and Training

Password management will be include in the Security Awareness and Training program which all personnel (employees, contractors and business associates) must attend at least once a year.

1.8 Network operating systems (OS)

OS operators must ensure that all operating systems password access have the following:

- Support authentication of individual and privileged users
- Not store passwords in clear text or in any easily reversible form. Using encryption/decryption features to protect the confidentiality of the passwords in storage and transmission for authentication
- Support TACACS+, RADIUS and/or X.509 with LDAP security retrieval, wherever possible

1.9 Enforcement

Passwords are to be systematically and automatically force end-user change at least every 90 days, not be reused for a set long duration, or easily guessed and bypassed or overwritten in any shape of form.

Any sharing or stealing of passwords or non-compliance to this password policy could result in employee sanctions or termination.

REFERENCES/SOURCES

HIPAA	ISO 27001
§ 164.308(a)(5) Security awareness and training	A.11.2.3 User password management
§ 164.308(a)(5)(ii)(D) Password management	A.11.3.1 Password use
§ 164.312(d) Password	http://csrc.nist.gov/publications/drafts/80

management	0-118/draft-sp800-118.pdf

POLICY HISTORY:

Supersedes: All previous Password Standard Policies
Date Reviewed: 12/18/2017
Date Revised: 12/18/2017