	POLICY Number: 7311-25-003 Title: Password Policy
Authorization [ ] President and CEO [X] Vice President, Finance and Corporate Services	Source: Director, Information Technology Services Cross Index: 7311-25-002, 7311-25-004 Date Approved: May 13, 2013 Date Revised: November 20, 2013 Date Effective: November 29, 2013 Date Reaffirmed: Scope: SHR & Affiliates

Overview

Passwords are a critical aspect of information and network security, providing the front line of protection for SHR User Accounts. A poorly created password could put all of SHR's electronic information at risk. As a result, it is important for SHR Users to take the appropriate steps to ensure they create strong, secure passwords for their SHR User Account, and to protect those passwords from improper use or compromise. This rule applies for each system/application that a user has been granted access to.

DEFINITIONS

Saskatoon Health Region (SHR) User means a person with an active SHR User Account that allows access to the SHR computer network. A SHR User may include SHR employees, affiliate employees, physicians, other healthcare professionals, students, contractors, vendors and any other person who has been approved for an SHR User Account.

Saskatoon Health Region (SHR) User Account means a personal account, consisting of an Active Directory username and a password that is granted user access privileges as specified on the *SHR User Account Application Form*. Privileges may include access to shared files, email and/or systems/applications.

1. PURPOSE

The purpose of this policy is to establish SHR's password requirements.

2. PRINCIPLE

Passwords ensure the security of SHR networks, resources, systems/applications and information, and protect these assets from unauthorized access and use.

3. POLICY

3.1 General

3.1.1 SHR User Account and system/application passwords must be unique.

3.1.2 Do not use the same password for both application/system user accounts and your SHR User Account.

3.1.3 Internet-exposed or DMZ (Demilitarized Zone) administrative account passwords must be different than internal administrative passwords. This will prevent internal accounts from being compromised if passwords of external-facing systems or services are cracked.

3.1.4 All SHR Business Unit application owners who are responsible for password security of the assigned system/application must comply with this policy. Any legacy (existing) systems/applications that cannot conform to all of the password standards must be configured to meet as many as possible.

3.1.5 All SHR system/application and SHR User Account passwords must be changed every four (4) months.

Exceptions:

3.1.1.1 Administrative passwords may be changed every six (6) months; however, in addition to following all the rules of regular passwords they must be at least twelve characters in length.

3.1.1.2 Automated service account passwords must be at least fifteen characters in length. Due to complex operational dependencies, this category of passwords will be changed at the discretion of IT Security as operational realities permit.

3.1.6 SHR Users shall be notified, two weeks in advance, of each password expiration and prompted to create a new password.

3.1.7 All suspected or confirmed instances of password compromise must be reported (see procedure 3.4).

3.2 Password Creation

3.2.1 Passwords ***must:***

- Be at least eight characters in length
- Contain characters from three of the following four categories:
  1. English uppercase characters (A through Z)
  2. English lowercase characters (a through z)
  3. Numbers (0 through9)
  4. Non-alphanumeric characters (e.g., !, $, #, %)

3.2.2 Passwords ***must not*** be:

- Based on a user's personal information or that of his or her friends, family members, or pets. Personal information includes logon ID, name, birthday, address, phone number, social insurance number, or any permutations thereof.
- Any part of the user's account name.
- Any one of the previous five passwords.
- Words that can be found in a standard dictionary (English or foreign) or are publicly known slang or jargon.
- Common usage words such as computer terms and names, commands, sites, companies, hardware, software, etc.
- Based on publicly known persons, or fictional characters from books, films, etc.
- Based on the SHR name or geographic location.

3.3 Password Protection

3.3.1 SHR Users shall not keep an insecure written record of his or her passwords, either on **paper** or in an electronic file. If it proves necessary to keep a record of a password, then this record must be kept in a secure place that only the user can access (if in hard copy form) or in an encrypted file (if in electronic form).

3.3.2 SHR Users shall treat passwords as confidential information. No employee, under any circumstance, is to give, tell, or hint at their password to another person, including ITS staff, administrators, managers, supervisors, other co-workers, friends, or family members. If someone demands a SHR User's password, refer them to this policy and your manager.

3.3.3 Passwords must not be:

- Transmitted electronically over the Internet.
- Inserted into email messages or other forms of electronic communication. (An exception to this rule is when passwords for new accounts are communicated via email between SHR email addresses.)
- Revealed on questionnaires or security forms.

3.3.4 The same password must not be used:

- To access SHR systems/applications and used to access non¬-SHR accounts or information. Example: Do not use the same password for SHR accounts as for a personal email account, personal banking, etc.
- To access multiple SHR applications. Example: Do not use one password for all business and clinical application unless this is done automatically (e.g. the applications are linked to your SHR User Account credentials).
- To access multiple SHR systems. Example: Do not use one password for both a SHR User Account and a UNIX user account.

3.3.5 SHR Users shall not use the "Remember Password" feature. This feature (also sometimes referred to as "Remember Me") is available on some internal and external (e.g. Internet) applications so that users do not have to re-enter their username and/or password the next time they visit. While convenient, this feature totally removes a user's access control restrictions, leaving them open to other users impersonating them, performing improper or embarrassing actions, and/or accessing information without their knowledge or consent.

4. ROLES AND RESPONSIBILITIES

4.1 SHR Users

4.1.1 Create a secure, confidential and safeguarded passwords according to the requirements set forth in this policy.

4.1.2 Reset forgotten passwords using built-in self-serve password reset functions whenever possible.

4.1.3 Immediately change a password and report the incident to their manager if they either know or suspect that his/her password has been compromised.

4.2 Managers

4.2.1 Ensure SHR Users have read, understand, and abide by the provisions of this policy.

4.2.2 Immediately report incidents of known or suspected password compromise to the ITS Service Desk at 655-8200 (or 1-866-431-1780 from the rural areas).

5. POLICY MANAGEMENT

The management of this policy including policy education, monitoring, implementation and amendment is the responsibility of the Director, Information Technology Services.

6. NON-COMPLIANCE/BREACH

Non-compliance with this policy will result in a review of the incident. A review for non-compliance may result in disciplinary action, up to and including termination of employment and/or privileges with SHR.

PROCEDURE Number: 7311-25-003 Title: Passwords	
Authorization [ ] President and CEO [X] Vice President, Finance and Corporate Services	Source: Director, Information Technology Services Cross Index: 7311-25-002, 7311-25-004 Date Approved: May 13, 2013 Date Revised: November 20, 2013 Date Effective: November 29, 2013 Date Reaffirmed: Scope: SHR & Affiliates

1. PURPOSE

The purpose of this procedure is to establish the processes related to password creation, protection, and reset, as well as explain how to report actual or suspected incidents of password compromise.

2. PRINCIPLE

Passwords are used to access any number of SHR systems/applications, including the network and voicemail. Weak passwords are easily cracked, and put the entire system at risk.

3. PROCEDURE

3.1 Create passwords that meet the requirements established by in this policy (see Policy section 3.2).

3.1.1 Create a password that is easy to remember but difficult to guess.
One way to do this is to create a password based on a song title, affirmation, or other phrase.

Example: If the phrase is "This May Be One Way To Remember", the password could be "TmB1w2R!" or "Tmb1W>r~" or some other variation.

NOTE: Do not use either of these examples as passwords!

3.2 Use and protect passwords appropriately (see policy 3.3).

3.2.1 If four attempts to access a SHR User Account are unsuccessful, the account is automatically suspended for15 minutes. Wait 15 minutes and try again.

3.3 Reset forgotten passwords using built-in self-serve password reset functions whenever possible. This is quicker and more efficient. [For instructions on how to do this, please refer to the guide How to: Forefront Identity Manager & Self-Service Password Reset on the "Self Help" page of the ITS InfoNet.]

Only if this feature does not work shall the user phone the ITS Service Desk at 655-8200 (1-866-431-1780 in the rural areas) for assistance.

3.4 If a SHR User either knows or suspects that his/her password has been compromised:

3.4.1 Change password immediately

3.4.2 Report incident to their manager

3.4.3 Manager reports incident to ITS Service Desk.

4. PROCEDURE MANAGEMENT

The management of this procedure including procedure education, monitoring, implementation and amendment is the responsibility of the Director, Information Technology Services.

5. NON-COMPLIANCE/BREACH

Non-compliance with this procedure will result in a review of the incident. A review for non-compliance may result in disciplinary action, up to and including termination of employment and/or privileges with SHR.