SCHARP | Atlas Password Policy

1 Purpose

The purpose of this policy is to protect data on the Atlas Science Portal from unauthorized access by describing and enforcing password selection and maintenance for the Atlas Science Portal.

2 Scope

The Atlas Science Portal allows authentication by 2 means: (1) SCHARP accounts and (2) Atlas-only accounts. This policy applies to anyone accessing or utilizing protected resources on the Atlas Science Portal by way of an Atlas-only account. Public access to the Atlas Science Portal does not require an account.

Atlas-only accounts constitute the majority of accounts. If you are not an employee of SCHARP, you most likely have an Atlas-only account.

SCHARP accounts (xyz@scharp.org) are for SCHARP employees only and are managed separately from Atlas-only accounts. SCHARP accounts are linked to an FHCRC HutchNet ID and subject to the FHCRC Password Policy. Please note that FHCRC email usernames (xyz@fhcrc.org) are not SCHARP accounts, they are Atlas-only accounts and are subject to this policy.

3 Policy

In general, a password's strength and effectiveness will increase with length, uniqueness and frequency of changes. These three items help defend against dictionary attacks and brute force attacks. In addition, account lockout settings are designed to help prevent a brute force attack on user passwords. A dictionary attack occurs when a malicious user tries known words that are in a dictionary to try and guess a password. A brute force attack occurs when a malicious user tries all of the possible permutations until one is successful.

3.1 Strong Passwords

- All passwords must meet the following minimum standards:
    - Must be eight characters or more.
    - Must contain three of the following: lowercase letter (a-z), uppercase letter (A-Z), digit (0-9), or symbol (e.g., ! # $ % & / < = > ? @).
    - Must not contain a sequence of three or more characters from your email address, display name, first name, or last name.
    - Must not match any of your 10 previously used passwords.

- To help prevent identity theft, personal or fiscally useful information such as birth date, Social Security or credit card numbers must never be used as a password.

3.2 Password Expiration

Passwords will expire 6 months after the last date they are changed. When a password expires, on login a system prompt will require the user to change their password. Failure to do so will prevent access to the Atlas Science Portal until the password has been changed.

3.3 Password Management Expectations

- Passwords are to be treated as sensitive information and should therefore never be written down unless adequately secured.
- Passwords should not be inserted into email messages or other forms of electronic communication.
- Passwords should not be shared with anyone.
- If you suspect your password has been compromised, please report the incident to atlas@scharp.org immediately. A password reset will be initiated for you, the incident will be logged, and system usage may be reviewed.

4 Enforcement

Any user found to have violated this policy or whose password may have been compromised may have their account disabled. If you’re account has been disabled, please contact atlas@scharp.org.

The Atlas Team manages the operations of the Atlas Science Portal and is responsible for enforcing this policy.