SCHARP | Atlas Account Policy

1 Purpose

The purpose of this policy is to protect data on the Atlas Science Portal from unauthorized access by establishing a standard for the administration of accounts that provide access to the Atlas Science Portal. An account consists of an email and a password, with access to some set of services and resources. This policy establishes standards for issuing and disabling accounts.

2 Scope

This policy applies to anyone accessing or utilizing protected resources on the Atlas Science Portal. Public access to the Atlas Science Portal does not require an account.

3 Policy

3.1 Issuing Accounts

- All Atlas account requests must come from, or be approved by, an Account Sponsor who must be one of the following:
    - A SCHARP Project or Program Manager
    - An established Network Specific Liaison
    - An established Lab Contact
    - The CAVD Portal Liaison
- Requests for access should go to atlas@scharp.org and include the Account Holder, the Account Sponsor, the level of permissions required, and the project folder(s) for which the Account Holder will need access to.
- The Account Sponsor assumes responsibility for the permissions granted to the Account Holder.
- The date when an account is issued will be logged in Atlas and available for audit.

3.2 Disabling Accounts

- Account Sponsors may request that an account issued under their request be disabled at any time.
- The Atlas Team reserves the right to disable an account for any reason, including:
    - Account inactivity for more than 1 year
    - Compromised password
    - Suspicious account activity
    - Inappropriate behavior in collaborative areas (e.g., wikis, forums)
- When an account has been disabled due to inactivity, the Atlas Team will notify the Account Holder by email after their account has been disabled.
- Disabled accounts may be re-enabled after review by contacting atlas@scharp.org.

3.3 Shared Accounts

Sharing of Atlas accounts is not allowed.

However, in some situations, a provision to support the functionality of a process, system, or application may be made. In this case, each shared account must have a designated owner who is responsible for the management of access to that account. Such exceptions also require documentation from the designated owner that justifies the need for a shared account, including a list of individuals who have access to the shared account. This documentation must be submitted to atlas@scharp.org for approval, and be made available upon request for an audit or a security assessment.

4 Enforcement

Any user found to have violated this policy 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.