1. Purpose

The purpose of this policy is to establish a standard for the secure use and protection of all work-related passwords.

2. Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any ALPHA facility, has access to the ALPHA network, or stores any non-public ALPHA Information.

3. Policy

3.1 Password Creation and Use

3.1.1 Users must use a separate, unique password for each of their work-related accounts. Users may not use any work-related passwords for their own personal accounts.
3.1.2 Staff are allowed to use authorized, approved password managers to securely store and manage all their work-related passwords.

3.2 Password Change

3.2.1 Passwords should be changed only when there is reason to believe a password has been compromised or fails to meet our Password Creation Requirements.

3.3 Password Protection

3.3.1 Passwords must not be shared with anyone, including supervisors and coworkers.
3.3.2 Passwords must not be inserted into email messages or other forms of electronic communication, nor revealed over the phone to anyone.
3.3.5 Any individual suspecting that their password may have been compromised must report the incident and change all relevant passwords.

3.4 Multi-Factor Authentication

3.4.1 Multi-factor authentication is highly encouraged and should be used whenever possible, not only for work related accounts but personal accounts also.

4. Responsibilities

The IT department of ALPHA is responsible for administering, maintaining and updating this policy with the approval of the chief technology officer, chief information officer and/or chief operating officer.

5. Compliance

5.1 Compliance Measurement

The IT team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the IT team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action

1. Purpose

This policy ensures the confidentiality, integrity and availability of data stored, accessed and manipulated using cloud computing services.

2. Scope

The scope of this policy includes all data handling on any cloud systems that resides at any ALPHA facility, has access to the ALPHA network, or stores any non-public ALPHA Information. All services within the cloud environment that fall into this category will be subject to the requirements specified within this policy. Therefore, it applies to every server, database and other IT system that handles such data, including any device that is regularly used for email, web access or other work-related tasks.

3. Policy

3.1 All cloud-based services must be approved prior to acquisition and deployment. To ensure secure adoption and usage of cloud services.

3.2 The cloud security administrator and IT security manager must perform an inventory of cloud services in use at least quarterly.

3.3 Only the cloud-based solutions on the list of approved services specified by of Cloud Security Administrator may be used.

3.4 Data from the “Sensitive” tier of the Data Classification Policy shall be available at all times, per regulations, for discovery and audit. Cloud providers shall conform to these compliance requirements.

3.5 At the time of cloud service implementation and quarterly after that, the Cloud Security Administrator shall review each service-level agreement, as well as request and analyze the cloud provider’s security audits.

3.6 The organization shall put into place tools for centralized visibility of the cloud service infrastructure, such as cloud workload protection (CWP) tools. The tools shall offer traffic analysis, configuration monitoring and assessment, and alerts for configuration issues.

4. Responsibilities

4.1 Cloud Security Administrator

The person ultimately responsible for implementation, configuration and maintenance of cloud services security.

5. Compliance

5.1 Compliance Measurement

The Cloud Security Administrator will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Cloud Security Administrator in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action.