Password Policy

|  |  |
| --- | --- |
| Policy Area | IT Policy Library |
| Approved Date | December 31, 20XX |
| Approved By | Policy Committee |
| Effective Date | January 1, 20XX |
| Current Version | 1.0 |

# I. Overview

Computer accounts are used to grant access to ABC Company’s Information Systems. The process of creating, controlling, and monitoring computer accounts is extremely important to an overall security program.

# II. Purpose

Identification and authentication access controls play an important role in helping to protect Information Systems. The purpose of this policy is to protect Information Systems by defining requirements for new passwords and changes to passwords.

# III. Scope

This policy applies to all ABC Company Staff that utilize Information Systems with IDs and passwords (credentials). This policy applies whether Staff is using ABC Company Information Systems, Staff owned devices for Company approved work, or Staff use Information Systems of third party service providers for work related activities.

# IV. Policy

The Chief Security Officer (CSO) shall ensure:

* Policies and procedures manage the process of creating, changing, and safeguarding passwords/phrases
* Policies and procedures prevent staff from sharing passwords/phrases with others.
* Procedures advise staff to commit their passwords/phrases to memory and not allow them to be written down.
* Policies and procedures govern the password/phrase change frequency.
* Policies and procedures dictate when passwords/phrases must be supplemented with additional access controls such as tokens and biometric.

This Policy applies to all ABC Company related authentication activities including, but not limited to, the following:

* Administrator accounts.
* User accounts.
* Network infrastructure devices (e.g. firewalls, routers, wireless access points, etc.).
* Third party service providers.
* Web applications.
* Screen savers.
* Mobile devices.

A. New User Accounts

When granting access for a new user/account:

* System administrators will establish a unique ID and unique password/phrase.
* The user password will be conveyed to the user in a secure manner.
* When the user logs on for the first time, the user will be required to change their initial password/phrase to something that meets the requirements of this policy.

B. Selecting Passwords/Phrases

The Chief Security Officer, working with the appropriate Data Owners, will determine the appropriate authentication methods to be used. In general, there are two options:

* Passwords change frequently. In this approach, passwords change every 90 days and users are not allowed to re-use the most recent 5 prior passwords. The advantage is that if someone becomes aware of a person’s password, they only have a short time (90 days) to use it. The disadvantage is that users may have a large number of passwords that expire on a frequent basis.
* Phrases are not required to be changed on a regular basis. Users are educated to choose phrases (memorized secrets) that are long and complex. Phrases are not the same as passwords. A phrase is a longer version of a password and is typically composed of multiple words. The phrase “We're off to see the wizard, The Wonderful Wizard of Oz” can be converted to WotstwTWWoO. By converting some letters to numbers and special characters the phrase is even more secure. With this option, systems and applications need to allow phrases up to 64 positions in length. Due to the possible length of the phrase, the Staff member shall have the option of seeing the phrase as it is entered, not just a series of asterisks or bullets.

Where possible, a password/phrase strength meter shall be used to help ensure Staff select long, strong, and complex passwords/phrases that meet the following requirements:

* Contain both upper and lower case characters (e.g., a-z, A-Z).
* Include both numbers (0-9) and special characters (e.g. @, #, $, \*).
* Have a minimum of at least 10 characters.
* Where possible, use different passwords/phrases for general office activities (e.g. e-mail, file access) vs. systems that store sensitive or confidential data.

Staff should not choose passwords/phrases that:

* Include common words such as those found in a dictionary.
* Are the same as passwords/phrases used on Staff personal accounts (e.g. personal e-mail, on-line banking, or social media).
* Contain personal information such as a spouse or pet’s name, social security number, driver's license number, street address, phone number, etc.
* Contain sequences or repeated characters. For example, 1234, 3333, abcdef, etc.
* Contain the name of the entity, application, or service.

Staff with special system privileges, assigned by a transaction, program, process, or group membership, should select a unique password/phrase from other accounts held by that individual.

C. Password/Phrase Guidelines

Staff shall follow security guidelines to ensure passwords/phrases are not compromised. Security training and awareness programs shall ensure Staff is:

* Educated on security related risks.
* Reminded of security requirements when selecting and protecting passwords/phrases.
* Educated not to select the "Remember Me" or “Remember Password” feature in web applications and browsers.
* Reminded to be careful when using social media so the password/phrase is not compromised.

Passwords/phrases must not be:

* Revealed to anyone.
* Stored, written down, or transmitted in clear (unencrypted) text.
* Inserted into unencrypted e-mail messages or other forms of electronic communications.

If a Staff member believes that their password/phrase has been compromised or made available to others, the Staff member must immediately change their password/phrase and notify IT security Staff.

If someone demands a password/phrase, refer them to this policy or have them contact the IT Department.

D. Password Changes

Passwords must be changed on a regular basis according to the following schedule:

* All administrator passwords must be changed at least every 30 days.
* All user passwords must be changed at least every 90 days.

When selecting a new password/phrase, Staff shall not repeat any of their prior five passwords/phrases.

E. Software Applications

Application developers must ensure programs contain the following security precautions:

* Applications must require each user to have their own unique ID (e.g. not shared, no user groups).
* Passwords/phrases and Sensitive Information must be protected using strong encryption.
* Passwords/phrases and Sensitive Information must not be transmitted or stored in clear text.
* Ensure applications timeout and require the user to enter a password/phrase after a period of inactivity.

# V. Enforcement

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

# VI. Distribution

This policy is to be distributed to all Staff members with access to ABC Company’s Information Resources.

**Policy History**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description | Approved By |
| 1.0 | 1/1/20XX | Initial policy release |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**References:**

COBIT APO01.03, APO01.11, APO12.02, APO13.07, DSS05.02, DSS05.07, MEA02.11

GDPR Article 25, 32

HIPAA 164.308(a)(1)(ii)(B), 164.308(a)(2), 164.308(a)(3)(ii)(A)

ISO 27001:2013 A9.3, A9.4

NIST SP 800-37 2.3

NIST SP 800-53 3.7, IA-2, IA-5

NIST Cybersecurity Framework PR.AC-1, PR.AC-3-4, PR.AC-7, DE.DP-2, RS.RP-1

PCI 2.1