Employee Password Policy

Cardinal Financial

Overview

At Cardinal Financial, we are committed to the preservation and confidence of company data. This password policy will ensure that all employees adhere to the objectives of keeping data available, accurate and confidential. To reduce risk of intrusion, this policy is a mandate for all employees and associates and applies to all connected networks , devices and computer systems.

User Password Guidelines Sec 1.0:

- passwords are to be at least 15 characters long; use of passphrases are highly encouraged
  - **passphrase defined per NIST SPF 800-63B**: A password that consists of a sequence of words or other text that a claimant uses to authenticate their identity. A passphrase is similar to a password in usage but is generally longer for added security
- passwords should be no longer than 64 characters long
- passwords do not require any special characters nor numbers
- passwords may not be shared with other employees or associates
- Passwords shall be changed every 90 days or forced change if any suspicious activity is indicated
- password age is set at 12 months for all employees and associates

Authentication Requirements Sec 1.2

To help verify identity, cardinal financial will use multi-factor authentication with the following requirements:

- all employees will be required to enter a one time passcode after entering their password before access is granted
- all employees will be issued a token to receive authentication codes or download the designated authenticator applicaton on a personal or company issued mobile device.
- a one time passcode will be generated by the authenticator and used only once to prove possession of the authenticator
- one time passcodes will expire after 7 minutes

Password Manager Use Guidelines Sec 1.3:

- password managers are provided and available for employees and associates to autofill password fields
- employees and associates can utilize password manager to generate a password that meets policy criteria, however employees and associates are also responsible for remembering password

Employee Responsibilities Sec 1.4

- passwords may not be shared with other employees or associates
- passwords must be safeguarded and not shared
- employees are responsible for creating and remembering passwords
- Loss of a authenticator token must be reported to the IT department immediately
- Employee must report any known or suspected password compromises
- passwords must not be shared in documents, files, nor emails
- upon resignation or termination, employees must return tokens to IT department

Evaluation and Review

This policy will be reviewed regularly to ensure its relevance and effectiveness in meeting company needs and compliance with current industry standards and best practices. Any changes or adjustments will be communicated to all employees.

Cardinal Financial, November 5, 2025

Briana A. Robinson
Information Security Officer

Employee Password Policy

Cardinal Financial