CITY OF SIGNAL HILL
Policy & Procedure

Multi-Factor Authentication Policy (MFA)

DATE: 6/7/2022

APPROVED: Hannah Shin-Heydorn

Attachment I

Multi-Factor Authentication Policy (MFA)

I. PURPOSE

The purpose of this policy is to provide guidance and define when the additional security provided by Multi-Factor Authentication (MFA) will be required to access City of Signal Hill ("City") network and email accounts. Every City of Signal Hill employee and elected or appointed officials are required to adhere to this Policy.

II. SCOPE

This policy applies to all users who access restricted or confidential data (or the systems that contain this data) maintained by the City. This policy applies to both on-site and off-site access to City resources whether the access is through City-owned or personally owned devices.

This policy applies to any system that contains confidential or restricted data or that requires an additional layer of protection as determined by the City Manager or City designated Information Technology Officer. Since Microsoft 365 services may hold restricted data these systems will be part of MFA.

III. DEFINITIONS

Multi-Factor Authentication (MFA): Method of authentication that requires more than one verification method. This adds a critical second layer of security when users sign-in to their City Office 365 account. It does this by requiring more than one method of verifying that it is really the user logging into the account.

User: Any person or entity accessing, logging into, or attempting to access or log into, a City hardware or software system; or connecting to, or attempting to connect to or traverse a City network, whether by hardware or software or both, from any location. The term "User" includes employee and elected or appointed officials, and any other individuals or agents who access and use City information technology.

Microsoft 365: Microsoft 365 is a suite of cloud-based solutions that includes Outlook email, SharePoint, and Teams.

IV. POLICY

With new technological advances it is easy for individuals to inadvertently fall victim to highly sophisticated phishing attacks. This could give a hacker unauthorized access to the City's network and information system (Network). The Administrative Services Department and Information Technology Services (IT) has taken several steps to protect and monitor the City's Network. As part of its efforts, IT has established a Multi-Factor Authentication Policy (MFA Policy), which provides a common method of protection for the City, that utilize and store sensitive personal, and financial information. In order to access City resources and the Network, all individuals will be required to engage in one additional step beyond the normal logon process. Individuals will be required to register a second approved device. The MFA system will send a message to the device which the individual must use to authenticate. Upon successful completion of this 2- step authentication process, the individual will be able to access the system.

All users who have access to confidential and/or restricted data will be required to use Multi-Factor Authentication on their City network and email accounts.

Users will be required to enroll a device to serve as the second authentication method as part of MFA. This second device can be an office phone, City provided cell phone, personal cell phone or supported authenticator app.

Users must contact IT to report suspicious activity or a compromised account.

Users understand they are required to re-authenticate their City accounts every 90 days. The City of Signal Hill does not require the use of a personal cell phone for multi-factor authentication. It is a user's choice if they wish to enroll and authorize a personal device as a method for multi-factor authentication as well as the user's responsibility to pay any charges related to such communications from the City.

Any users who do not authorize the City to text or communicate through a personal device as a method for multi-factor authentication may elect to use a City phone (DID or mobile) as the method of authentication. When a City DID phone is used as the sole method of MFA, the user understands they will not be able to access their accounts outside of their assigned, City secured facility workstation associated with the applicable City phone line.

V. PERIODIC REVIEW AND RECERTIFICATION

Due to the rapid change in technology and increase in cyber security threats, the content of this Policy is subject to regular review at the discretion of City Manager or City designated Information Technology Officer in collaboration with Information Technology Services.

City of Signal Hill
Multi-Factor Authentication Policy User Acknowledgement

I hereby acknowledge that I have read and understand the City's Multi-Factor Authentication Policy (MFA) and agree (as a user of the City's information technology) to the following additional security measures and protections to access the City's network.

- I agree to use MFA on my City accounts and understand that I am required to enroll a device of my choosing to serve as one of the following authentication communication methods as part of MFA.
    - Microsoft Authenticator Application
    - SMS/Text Message to a mobile device
    - Call to user phone (Office DID or Mobile)
- I understand that I must report suspicious activity or a compromised account to IT.
- I understand I am required to re-authenticate their City accounts every 90 days.
- I understand that I am not required to use my personal cell phone for multi-factor authentication and agree that it is my choice to enroll my personal device as an MFA communication method. I also agree that should I choose to enroll my personal device that any communication charges incurred related to MFA will be my responsibility to pay.
- I understand that when a City DID phone is used as the sole method of MFA, I will not be able to access my City account outside of the City secured facility workstation that is associated with the applicable City phone line.

□ **I accept the use of Multi-Factor Authentication.**

By signing below, I certify that I understand the City's policy and accept to use Multi-Factor Authentication on my City accounts to access the City's resources and Network.

Name (printed): ______________________________

Signature: __________________________________ Date: _______________