City of Forest Park

Multi-Factor Authentication (MFA) Policy

1. Purpose
This policy outlines the requirements and procedures for implementing multi-factor authentication (MFA) for all employees of the City of Forest Park. This policy is designed and intended to enhance the security of our systems and data.

2. Scope
This policy applies to all employees, contractors, and third-party vendors who access the City of Forest Park's systems and data. This policy will apply to all domain authentications including but limited to email, VPN connections, and computer logins.

3. Policy

3.1. MFA Requirement
All employees accessing the City of Forest Park's systems and data are required to use multi-factor authentication (MFA).

3.2. Authentication Device
Employees who possess a city-issued cell phone must use it as their primary authentication device to generate the MFA token.

3.3. Alternatives for Non-City Issued Phones
a. Employees who do not have a city-issued phone will be provided with an MFA fob as the token key.
b. Alternatively, employees without a city-issued phone may opt to use their personal smartphone as the authentication device. If the employee chooses to use a personal device for the MFA application, there

would be no expectation of reimbursement as this option is completely voluntary and only offered as a convenience.

3.4. Provisioning and Setup
a. The IT department is responsible for provisioning MFA accounts for all employees.
b. Employees will receive instructions from the IT department on how to set up and configure MFA on their chosen authentication device.
c. Employees must follow the setup instructions promptly upon receipt.

3.5. Compliance
a. Failure to comply with this policy may result in disciplinary action, up to and including termination of employment.
b. Exceptions to this policy must be approved by the Chief Information Officer along with the City Manager.

4. Responsibilities
a. IT Department: Responsible for provisioning MFA accounts, providing setup instructions, and ensuring compliance with this policy.
b. Employees: Required to set up and use as per the instructions provided by the IT department.

5. Enforcement
The IT department, in conjunction with HR, will periodically audit compliance with this policy. Non-compliance may result in appropriate disciplinary action.

6. Review and Revision
This policy will be reviewed annually and updated as necessary to reflect changes in technology, regulations, or organizational requirements.

7. Definitions
a. Multi-Factor Authentication (MFA): A security process that requires users to provide two or more forms of authentication to access systems or data.

8. Contact Information
For questions or concerns regarding this policy, please contact the IT department. The email address is techsupport@forestparkga.gov or you may call TECH (8324) from any City desk phone or 470-781-8500 if calling from a cell phone or outside of the City's network.