



A Century of Progress with Pride

MFA Security Verification Policy

1. Purpose

To enhance cybersecurity and protect company systems and data, all City employees are required to use Multi-Factor Authentication (MFA) for accessing City of Berwyn networks and systems. Multifactor authentication is a layered approach to securing data and applications where a system requires a user to present a combination of two or more credentials to verify a user's identity for login. MFA increases security because even if one credential becomes compromised, unauthorized users will be unable to meet the second authentication requirement and will not be able to access the targeted physical space, computing device, network, or database. This policy ensures secure access and mitigates unauthorized access risks.

2. Scope

This policy applies to all City employees with access to City systems that require authentication.

3. Policy Statement

1. Mandatory MFA Enrollment

- All employees must enroll their company-approved or personal cell phone with the current MFA provider to ensure functional multi-factor authentication is in place over their account(s). This includes the installation of the current MFA provider's mobile application on any city or personally-owned cell phone in the possession of the employee.
- Enrollment must be completed within **five (5) business days** of receiving system access credentials.

2. Device Requirements

- Employees must install the current MFA provider's Mobile app on a compatible smartphone (iOS or Android).
- The device must support push notifications and biometric verification where applicable.

3. Authentication Methods

- Employees must use the current MFA provider's push notification options (where available) as the primary authentication method.
- In cases where push notifications are unavailable, manual entry of the passcode from the current MFA provider's app is acceptable.

4. Security Compliance

- Employees must keep their MFA-enrolled device secured and report any loss or theft immediately to IT Security.
- Employees must not share or delegate MFA authentication to any other person.

5. Non-Compliance & Exceptions

- Failure to enroll in the current MFA provider within the required timeframe may result in account suspension until compliance is achieved.
- Employees who are unable to use the current MFA provider due to technical or accessibility reasons must request an exemption in writing to IT Security for review.

** As of April 2025, the current approved MFA provider for the City of Berwyn is **Duo** (<https://duo.com>), maintained by *Cisco Systems*. The City of Berwyn reserves the right to transition to another MFA platform at its discretion with the approval of the IT Security Analyst and IT management.**

As an employee of the city of Berwyn I acknowledge I have read the policy above, understand it and agree to abide by said policy.

Employee Name (Printed): _____

Employee Signature: _____

Date Received: ____/____/____

Star #, if applicable: _____

