NYC DOITT
Information Technology & Telecommunications

FAQ
Multi-Factor Authentication & the Microsoft Authenticator App

- **What is MFA?**
  Multifactor authentication (MFA) is a security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login or other transaction. Multifactor authentication combines two or more independent credentials: what the user knows (password), what the user has (mobile device) and what the user is (biometric verification). The goal of MFA is to create a layered defense and make it more difficult for an unauthorized person to access a target. If one factor is compromised or broken, the attacker still has at least one more barrier to breach before successfully breaking into the target.

- **Why are we doing this?**
  We hear about high profile security breaches frequently. Most of these breaches exploit the system login credentials of end users to get into the company's network. The City recognizes this and is focused on better securing end user identities. Multi-factor authentication (MFA) is one method for doing this as MFA requires a user to provide more than just a password to access the network. These additional factors of authentication require the user to provide something that only the user knows, has and is.

- **Where do I download the Authenticator App?**
  Android phones: https://go.microsoft.com/fwlink/?linkid=869516
  iOS phones: https://go.microsoft.com/fwlink/?linkid=869517
  Windows phones: https://go.microsoft.com/fwlink/?linkid=823234

- **What methods are available for me as a second factor?**
  The primary security verification will be to get notification through the MS Authenticator phone app; additional methods available are: to receive a call on your authentication phone, to receive a call on your office phone or to use a verification code from the MS Authenticator phone app.

- **Can I use authentication by text?**
  No. Text messages have a lot of security problems, and are the least secure option for two-factor authentication. If someone knows your phone number and can get access to personal information like the last four digits of your social security number—unfortunately, this be easy to find thanks to the many corporations and government agencies that have leaked customer data—they can contact your phone company and move your phone number to a new phone. This is known as a "SIM swap", and is the same process you perform when you purchase a new device and move your phone number to it.

- **What happens if I forget my mobile phone?**
  Call the service desk, verify who you are (preferably by providing your PIN – which can be set through NYC Password Self Service: https://nycpss.nycid.nycnet/sspr/private/Login), and the Service Desk agent will be able to allow you to bypass MFA for a short period of time, until you've recovered your mobile phone.

- **What happens if I lose my phone?**
  Call the service desk, verify who you are (preferably by providing your PIN – which can be set through NYC Password Self Service: https://nycpss.nycid.nycnet/sspr/private/Login), and the Service Desk agent will be able to disable MFA from the lost phone, allow you to bypass MFA for a short period of time, until you've found or replaced your lost phone, and reset your MFA so you can re-enroll from your replacement phone.

- **For which applications will I be required to two-factor authenticate?**
  Microsoft Outlook, desktop and online versions, SharePoint Online, Skype for Business, and One Drive

- **Will I have to two-factor authenticate each time I log into Microsoft Outlook desktop, SharePoint Online, Skype for Business, and One Drive from my office desk?**
  No, you will be prompted to two-factor authenticate when on premise once every 14 days (unless you switch computers, in which case you will be prompted on the new computer).

- **Is any information collected on my phone when using the MS Authenticator app?**
  No info is collected on your phone.

- **What do I do if my office phone is incorrect on the MFA enrollment site?**
  If your office phone, as displayed in the MS Azure MFA enrollment site is not accurate, enter your correct office phone number in the "Alternate Authentication phone #" field (Service Desk users should enter their correct office phone number in the "Authentication phone #" field).

- **What if I don't want to use my personal mobile phone for MFA?**
  You can enter your office phone # as the "Authentication phone #", however, you will not be able to access Office 365 applications remotely.

- **Will my home use of Microsoft Office be effected?**
  Your use of Microsoft Office on your home computer will not be effected unless you use your work email account as your Microsoft account for Microsoft Office applications at home.

- **How are accounts de-provisioned from MFA? Once a LAN account is de-provisioned/off-boarded, is there any MFA clean up needed by the Service Desk or the users Manager?**
  No special actions are needed.

- **When I open MS Outlook when using remote desktop, how come I'm asked to two-factor authenticate more often than once every 14 days?**
  Each time you use remote desktop, you may be hitting a different server each time, so the 14-day token may or may not be present on the server you happen to be using.

- **What do I do if I choose to use a code sent to my mobile phone for authentication but it does not work?**
  Try to re-install the MF Authenticator app on your phone; if the issue persists, call the Service Desk.

- **As many DoITT staff do not have DoITT-issued mobile devices, does DoITT's BYOD (Bring Your own Device) policy apply to personal devices on which the Microsoft Mobile Authenticator App is installed for work use?**
  Installing the Microsoft Mobile Authenticator App on your personal device, for work use, does not cause DoITT's Bring Your Own Device (BYOD) policy to apply to your personal device. The Microsoft *privacy statement*, however, does apply.