Microsoft Authenticator on Personal Devices
Frequently Asked Questions (FAQ)

1. Why do I need to use Microsoft Authenticator on my personal phone?

- Microsoft Authenticator provides secure multi-factor authentication (MFA), adding a critical layer of protection for your work accounts. Using it on your personal phone allows you to verify your identity quickly and securely, reducing the risk of unauthorized access.

2. Does my employer have access to my personal phone or data?

- No. Installing Microsoft Authenticator does not give your employer access to your personal apps, messages, photos, or other data. The app only verifies your identity when logging into work-related services.

3. Can Microsoft Authenticator track my location or activity?

- By default, Microsoft Authenticator does not track your location. However, if your organization enables location-based policies, it may request location verification only at the time of authentication and only for security purposes.

4. Will using the app drain my battery or slow down my phone?

- No. Microsoft Authenticator is lightweight and runs efficiently in the background, using minimal battery and processing power.

5. Is my personal information at risk if I use Microsoft Authenticator?

- No. The app does not collect personal information beyond what's needed to authenticate your work account. It's designed with security and privacy in mind and complies with Microsoft's data privacy standards.

6. What happens if I lose my phone?

- If your phone is lost or stolen, notify your IT department immediately (915-273-3301) or open an IT service ticket. They can help revoke access or reset MFA settings to prevent unauthorized access.

7. Can I uninstall Microsoft Authenticator after setup?

- You can uninstall the app, but it is not recommended since it may prevent you from accessing work systems that require MFA. You will need the Authenticator app every time when you log in to a county system needing MFA authentication.

8. Is using Microsoft Authenticator mandatory?

- Many organizations require MFA for security compliance. For now, Microsoft Authenticator is El Paso County's preferred MFA method. In some special cases, alternate MFA methods may be available based on legitimate business purposes. While the use of Microsoft Authenticator on personal devices is not currently enforced, policies and job descriptions are being updated to reflect the requirement for the use of personal devices to access EP County IT resources.

9. Will my device be subject to Open Records if I use Microsoft Authenticator?

- No, your personal device is not automatically subject to open records requests simply because you use Microsoft Authenticator.
- The Microsoft Authenticator app is used solely to verify your identity when accessing work systems. It does not store, transmit, or interact with work-related content or records that would be considered subject to public disclosure.

10. Do I need to use MFA when connecting to VPN?

11. Yes, this process is already in place. For details, refer Multi-Factor Authentication for VPN.

12. Do I have to enter this passcode every time I unlock my computer?

- You will only need to enter the passcode once per day on your computer.

13. Why do I have to enter the passcode multiple times in a day?

- There are some factors that may cause this but more commonly due to an internet outage.

14. What if I log into another user's computer?

- You will be required to enter your authentication passcode again, including when using Remote Desktop or logging in from a different workstation.

If you still need assistance setting up or Microsoft Authenticator, please contact the ITD Helpdesk:

- **Call:** 915-273-3307
- **Email:** helpdesk@epcounty.com
- **Visit:** elpaso.happyfox.com/new