Multi-Factor Authentication Setup Guide

This document provides a step-by-step guide to configure Multi-Factor Authentication (MFA) for organizational systems, helping enhance security through additional verification.

---

1. Prerequisites

- Access to your organizational account credentials.
- A mobile device (smartphone or tablet).
- An authenticator app (such as Microsoft Authenticator, Google Authenticator, or Authy).
- Administrative access (if setup is organization-wide).

2. MFA Setup Steps

1. **Login to Your Account**
    - Visit your organization's authentication portal and log in with your username and password.
2. **Access Security Settings**
    - Navigate to `Account Settings > Security` or equivalent menu.
3. **Choose Multi-Factor Authentication Option**
    - Select `Enable Multi-Factor Authentication` or `Set Up MFA`.
4. **Select Authentication Method**
    - Choose your preferred MFA method:
        - Authenticator App (recommended)
        - SMS-based codes
        - Hardware token (if applicable)
5. **Link Authenticator**
    - Open the authenticator app on your device.
    - Scan the QR code displayed on the setup page *(or manually enter the setup key if prompted)*.
6. **Enter Verification Code**
    - Type in the code generated by your authenticator app to verify the configuration.
7. **Save Recovery Codes**
    - Download or copy backup/recovery codes and store them securely.
8. **Complete Setup**
    - Review your setup and confirm the activation of MFA on your account.

---

3. Troubleshooting & Tips

- Keep backup codes in a safe, offline location.
- If you lose access to your device, use recovery options or contact your administrator.

- Regularly review your authentication methods for outdated or unused devices.

> *For organization-wide enforcement, contact your IT administrator to enable and monitor MFA settings through the central admin console.*