**Company K Two-Factor Authentication Setup**

**1. Purpose**

This document outlines the procedures for setting up and using Two-Factor Authentication (2FA) at Company K. The goal is to enhance security by requiring a second form of verification in addition to the standard password, reducing the risk of unauthorized access to company accounts and systems.

**2. Scope**

This policy applies to all employees, contractors, and third-party collaborators who access Company K’s systems, applications, or networks that support Two-Factor Authentication.

### **3. Overview of Two-Factor Authentication**

Two-Factor Authentication (2FA) adds an extra layer of security by requiring users to provide two forms of identification:

1. **Something You Know**: Your password or PIN.
2. **Something You Have**: A verification code generated by a device (e.g., smartphone) or sent via SMS.

This ensures that even if a password is compromised, unauthorized access is still prevented without the second factor.

### **4. Setting Up Two-Factor Authentication**

**4.1 Prerequisites**

* Ensure you have a compatible device for receiving or generating 2FA codes (e.g., smartphone with an authenticator app, mobile phone for SMS).
* Have your Company K credentials (username and password) ready.

#### **4.2 Enabling 2FA for Company K Accounts**

1. **Log In to Your Account**
   * Visit the Company K account login page and sign in with your username and password.
2. **Access Security Settings**
   * Navigate to the security settings or account settings section of your account profile.
3. **Select Two-Factor Authentication**
   * Look for the option to enable Two-Factor Authentication. This might be under a section titled “Security” or “Authentication.”
4. **Choose Your 2FA Method**
   * **Authenticator App**: Choose this method if you prefer to use an app that generates time-based one-time passwords (TOTPs). Popular apps include Google Authenticator, Microsoft Authenticator, and Authy.
   * **SMS/Text Message**: Choose this method if you prefer to receive verification codes via SMS.
5. **Setup Process  
   For Authenticator Apps:**
   * **Install an Authenticator App**: Download and install an authenticator app on your smartphone.
   * **Scan QR Code**: Use the app to scan the QR code displayed on the setup page.
   * **Enter Code**: The app will generate a verification code. Enter this code on the setup page to complete the process.
6. **For SMS/Text Messages:**
   * **Enter Phone Number**: Input your mobile phone number where you wish to receive verification codes.
   * **Receive Code**: A verification code will be sent to your phone via SMS.
   * **Enter Code**: Input the code received on the setup page to complete the process.
7. **Backup Codes**
   * Once 2FA is set up, you may be provided with backup codes. Save these codes in a secure location. They can be used if you lose access to your primary 2FA method (e.g., if your phone is lost or damaged).
8. **Verify Setup**
   * Log out of your account and log back in to test that 2FA is working correctly. You should be prompted to enter a verification code in addition to your password.

### **5. Using Two-Factor Authentication**

**5.1 Logging In with 2FA**

* Enter your username and password on the login page.
* You will be prompted to enter a verification code.
* Open your authenticator app or check your SMS for the code and enter it into the provided field.
* Access will be granted if the code is correct.

**5.2 Recovering Your Account**

If you lose access to your 2FA method:

1. **Use Backup Codes**: If you have backup codes, use one of them to access your account.
2. **Contact IT Support**: If you do not have backup codes or need additional assistance, contact the IT Support team at **it-support@companyk.com** for help with account recovery.

### **6. Best Practices for Two-Factor Authentication**

* **Keep Your Device Secure**: Ensure that the device used for receiving or generating 2FA codes is secure. Use a password or biometric lock on your device.
* **Update Your Contact Information**: Ensure your mobile phone number is up-to-date in case you use SMS for 2FA.
* **Be Cautious with Backup Codes**: Store backup codes in a secure place, separate from your primary 2FA device.

### **7. Troubleshooting**

**7.1 Common Issues**

* **Authenticator App Not Generating Codes**: Ensure the time on your phone is correctly synchronized. Some apps require accurate time settings to generate valid codes.
* **SMS Code Not Received**: Check if your phone has signal or try restarting your phone. Contact IT Support if the issue persists.

**7.2 Contact IT Support**

For any issues related to 2FA setup or usage, please contact:

* **Email**: it-support@companyk.com
* **Phone**: [IT Support Hotline Number]

### **8. Policy and Compliance**

All employees are required to use Two-Factor Authentication for accessing Company K systems and applications where it is enabled. Non-compliance with the 2FA policy may result in restricted access or other disciplinary actions.