**Company K VPN Setup and Connectivity**

**1. Purpose**

The purpose of this policy is to outline the procedures for setting up and connecting to the Company K Virtual Private Network (VPN). The VPN allows employees to securely access Company K’s internal network and resources remotely. This policy ensures that all connections are secure, compliant with IT standards, and minimize the risk of unauthorized access.

**2. Scope**

This policy applies to all employees, contractors, and third parties who require remote access to Company K’s internal systems and resources. It covers the requirements for VPN usage, setup instructions, connectivity troubleshooting, and security guidelines.

### **VPN Usage Guidelines**

**3. Authorized Use**

* **Employee Access:** Only authorized employees, contractors, and partners may use the VPN to access Company K’s network. Approval must be obtained from the IT department.
* **Access Rights:** VPN access will be granted based on the employee’s role and business requirements. Sensitive systems and databases may require additional security measures.
* **Data Encryption:** All data transmitted over the VPN will be encrypted to protect sensitive information from being intercepted by unauthorized parties.

**4. VPN Security**

* **Strong Authentication:** All VPN users must use a unique username and strong password, following Company K’s password management policy.
* **Two-Factor Authentication (2FA):** Two-factor authentication is required for VPN access to provide an additional layer of security. Employees will need both their password and a one-time code sent to their mobile device or email.
* **Device Security:** Only company-approved and secure devices may connect to the VPN. Personal devices must meet security standards set by IT, including up-to-date antivirus software and a secure firewall.
* **Connection Timeouts:** Inactive VPN sessions will be automatically disconnected after a specified period to reduce the risk of unauthorized access.

### **VPN Setup Instructions**

**5. VPN Software Installation**

* **Step 1: Request VPN Access:**
  + Employees must submit a request to the IT department to obtain VPN access.
* **Step 2: VPN Client Installation:**
  + **Windows/Mac:** IT will provide access to the approved VPN client software. Download and install the VPN client on your device.
  + **Mobile Devices:** For smartphones or tablets, the VPN client is available through the Apple App Store (iOS) or Google Play Store (Android).
* **Step 3: Configuration:**
  + IT will provide configuration details, including the VPN server address, port number, and encryption settings. These details must be entered into the VPN client software.

**6. Connecting to the VPN**

* **Step 1: Open the VPN Client:**
  + Launch the VPN software on your device.
* **Step 2: Enter Credentials:**
  + Enter your username and password provided by IT. You will also be prompted for a two-factor authentication code.
* **Step 3: Connect:**
  + Click the “Connect” button to establish a secure VPN connection to the Company K network. You will see a notification once the connection is successful.
* **Step 4: Verify Connection:**
  + Once connected, you will be able to access Company K’s internal resources such as shared drives, internal applications, and databases.

**7. Disconnecting from the VPN**

* **Step 1: Close Connection:**
  + When finished, disconnect from the VPN by clicking the “Disconnect” button in the VPN client.
* **Step 2: Log Out:**
  + Always log out of any internal systems or applications before disconnecting from the VPN to ensure that your session is securely closed.

### **VPN Connectivity Troubleshooting**

**8. Common Issues and Resolutions**

* **Unable to Connect:**
  + Verify that your internet connection is active. If the issue persists, restart your VPN client or reboot your device.
* **Authentication Failed:**
  + Ensure that you are entering the correct username and password. If you have forgotten your credentials, contact the IT help desk to reset your password.
* **Connection Drops Frequently:**
  + Check your network stability. If using Wi-Fi, try moving closer to your router or switching to a wired connection.
  + Ensure that your VPN client is up to date. IT may also provide additional troubleshooting if network issues persist.
* **2FA Code Not Received:**
  + Ensure that your mobile device is receiving network signals or is connected to Wi-Fi. Resend the code if necessary, or contact IT if the issue persists.

**9. Support**

* For assistance with VPN installation, configuration, or connectivity issues, employees can contact the IT help desk at [IT Support Contact Information].
* IT may provide remote troubleshooting and assist with network diagnostics to resolve any issues related to VPN access.

### **VPN Security Best Practices**

**10. Secure Use of VPN**

* **Public Wi-Fi:** Employees are advised to avoid using public Wi-Fi networks when accessing the VPN, as these networks may be insecure. If public Wi-Fi must be used, employees should ensure their device firewall is enabled and that they log out immediately after use.
* **Device Protection:** Employees must ensure that their devices are updated with the latest operating system patches and have antivirus software enabled. IT may provide guidance on required security software.
* **Unauthorized Access:** Employees must report any suspicious activity or unauthorized access to their VPN account immediately to IT. Regular monitoring of access logs will be performed by IT to detect anomalies.

**11. VPN Usage Monitoring**

Company K’s IT department reserves the right to monitor VPN activity to ensure compliance with security protocols. VPN logs will be reviewed periodically to identify any unauthorized or suspicious access. Any violations of this policy will result in appropriate action, including the potential revocation of VPN privileges.

### **Policy Review**

**12. Annual Review**

This policy will be reviewed annually to ensure it remains aligned with current security standards and best practices. Updates will be communicated to all employees, and IT will provide training on new procedures if necessary.

**13. Contact Information**

For VPN setup, connectivity issues, or security concerns, employees can contact the IT department at it@companyk.com or submit a support ticket through the Company K internal portal.