**Company K Password Management and Reset**

**1. Purpose**

The purpose of this policy is to provide guidelines for secure password management and the process for resetting forgotten or compromised passwords. The goal is to ensure that employees maintain strong password practices and are able to reset their passwords safely and efficiently.

**2. Scope**

This policy applies to all employees of Company K who have access to any company systems, tools, or third-party portals. It covers password creation, management, and the process for resetting passwords when necessary.

### **Password Management Guidelines**

**3. Password Creation Requirements**

To maintain the security of Company K systems, all employee passwords must meet the following requirements:

* **Length:** Passwords must be at least 12 characters long.
* **Complexity:** Passwords must contain a mix of uppercase and lowercase letters, numbers, and special characters.
* **Avoid Common Words:** Passwords must not include easily guessable information such as “password,” names, or dictionary words.
* **Unique Passwords:** Employees must use unique passwords for each system or account and avoid reusing passwords from personal accounts.
* **Two-Factor Authentication (2FA):** Employees are required to enable two-factor authentication where available, particularly for sensitive systems or accounts.

**4. Password Storage and Protection**

* **Do Not Share Passwords:** Employees must not share their passwords with others, including coworkers or supervisors.
* **Secure Storage:** If employees need to store passwords, they must use a secure password manager. Writing down passwords on paper or storing them in unencrypted files is prohibited.
* **Regular Updates:** Employees are encouraged to update their passwords every 90 days to enhance security.

### **Password Reset Process**

**5. Forgot Password Process for Company K Systems**

If an employee forgets their password or suspects that their password has been compromised, they must follow the password reset process outlined below:

* **Step 1: Initiate Password Reset:**
  + Go to the Company K login page and click on the “Forgot Password” link.
* **Step 2: Verification:**
  + Enter your registered email address or username.
  + A verification code will be sent to your registered email or phone number.
* **Step 3: Enter Verification Code:**
  + Enter the code received via email or SMS in the designated field on the reset page.
* **Step 4: Create a New Password:**
  + Once verified, you will be prompted to create a new password. Ensure that it follows the password creation requirements outlined above.
* **Step 5: Confirm and Log In:**
  + After successfully resetting the password, log in using the new password and update any password-storing systems (such as a password manager).

**6. Example Reset Process for Popular Portals**

Below are examples of password reset processes for popular portals that Company K may use:

**a. Microsoft Office 365:**

* **Step 1: Go to Office 365 Sign-In Page:**
  + Navigate to the Office 365 login page:<https://office.com>.
* **Step 2: Click "Can't access your account?":**
  + Click on the “Can’t access your account?” link under the sign-in box.
* **Step 3: Select Account Type:**
  + Choose “Work or school account” for Company K users.
* **Step 4: Enter Email Address:**
  + Enter your Company K email address and the characters displayed in the CAPTCHA.
* **Step 5: Verify Identity:**
  + Select how you want to receive a verification code (email, SMS, or authentication app).
* **Step 6: Enter Verification Code:**
  + Enter the code you received to verify your identity.
* **Step 7: Create a New Password:**
  + Create a new, secure password and confirm. You will be redirected to the sign-in page once complete.

**b. Google Workspace (Gmail, Drive, etc.):**

* **Step 1: Go to Google Account Recovery Page:**
  + Visit the Google Account Recovery page: https://accounts.google.com/signin/recovery.
* **Step 2: Enter Email Address:**
  + Enter your Company K Google Workspace email address.
* **Step 3: Verification Options:**
  + Google will provide several options for account verification, such as sending a code to your registered phone number or answering security questions.
* **Step 4: Enter Verification Code:**
  + Enter the verification code received and proceed to the next step.
* **Step 5: Set New Password:**
  + Once verified, set a new password following the guidelines provided by Google.
* **Step 6: Confirm and Log In:**
  + Log in with your new password and confirm that everything is functioning correctly.

**7. Compromised Passwords**

* **Immediate Action:**
  + If an employee believes their password has been compromised, they must reset it immediately using the process outlined above.
* **Notify IT:**
  + Employees must notify the IT department if they suspect unauthorized access to any Company K systems or accounts, so IT can monitor for potential security breaches.
* **System Lockdown (if necessary):**
  + If a security breach is confirmed, IT may temporarily lock access to affected systems until the issue is resolved.

### **Enforcement and Violations**

**8. Monitoring and Compliance**

* **Monitoring:** Company K’s IT department monitors for suspicious activity, including multiple failed login attempts or unusual access patterns, which may indicate compromised accounts.
* **Violation of Policy:** Employees found violating this password management policy may face disciplinary action, up to and including termination, depending on the severity of the breach.

**9. Policy Review**

This policy will be reviewed annually to ensure it aligns with the latest security best practices and complies with evolving cybersecurity regulations. Updates will be communicated to all employees.

**10. Contact Information**

For assistance with password resets or security concerns, employees can contact the IT help desk at [IT Contact Information] or submit a support ticket through the company’s internal portal.