KECK GRADUATE INSTITUTE

A Member of The Claremont Colleges

Password Policy

Purpose

This Password Management Policy outlines the guidelines and procedures for creating, managing, and protecting passwords within Keck Graduate Institute (KGI). Passwords are crucial components of our cybersecurity framework, and adhering to these guidelines is essential for safeguarding our institution's sensitive information and assets.

Applies To

All users, including contractors and vendors with access to KGI's systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

The COO and the Office of Information Technology Services are responsible for ensuring policy compliance on systems owned or managed by KGI. Cabinet and Department heads are responsible for providing policy compliance within their respective areas.

Policy Guidelines:

1. **Password Creation:**

   a. Employees must create strong passwords that are at least 12 characters long.
   b. Passwords must include a combination of uppercase and lowercase letters, numbers, and special characters. (e.g. ~!@#$%^&*(){}|:"<>?,./[])
   c. Employees are prohibited from using easily guessable passwords such as "password," "123456," or common words.
   d. Passwords should not contain personal information such as birthdays, names, or significant dates.

2. **Password Storage & Sharing:**

   a. Passwords must not be stored in plaintext or shared through insecure communication channels such as email or messaging apps.
   b. Employees are strictly prohibited from sharing passwords with colleagues, vendors, or external parties.
   c. Each employee is responsible for maintaining the confidentiality of their passwords and accounts.

3. **Password Usage:**

a. Employees must not use the same password for multiple accounts or systems.
b. When accessing KGI systems or resources remotely, employees must ensure secure connections, such as VPNs, and refrain from saving passwords on public or shared devices.

4. **Password Security:**

a. Employees should be vigilant against phishing attempts or social engineering attacks that aim to obtain passwords illicitly.
a. In case of suspected or confirmed password compromise, employees must report it immediately to the IT department for investigation and remediation.
b. Multi-factor authentication (MFA) should be implemented wherever possible to add an extra layer of security to password-protected accounts and systems.

Policy Review

The IT department will review this Password Management Policy annually in consultation with relevant stakeholders to ensure its effectiveness and relevance in mitigating cybersecurity risks.

Adherence to this policy is essential for maintaining the integrity and security of KGI's digital assets and infrastructure. All employees must familiarize themselves with this policy and strictly adhere to its guidelines.

Contacts

IT Help Desk @ helpdesk@kgi.edu

Policy Version History

Version	Date	Description	Approved By
1.0	05/10/2024	Initial Policy	Cabinet
2.0	06/04/2025	Changed template and added version history.	VP of Finance & Administration

Responsible Officer – Vice President of Finance & Administration

Administrator – Information Technology Department