YPICS PASSWORD POLICY

DOCUMENT TABLE OF CONTENTS:

SUMMARY

All YPICS staff members are required to use a strong password that is 8-24 characters long in addition to Google's 2 Step Verification (2SV). All YPICS students are required to use a strong password that is 8-24 characters. Staff and students will be asked to conduct an annual reset of their password every 365 days. Any active YPICS Google account that has not logged in during the past 45 days will be suspended until we can verify the identity of the staff or student

WHY BEHIND POLICY

Below are some of the reasons why all YPICS Staff and students are required to use a strong password for their YPICS Google Accounts.

- The more characters your password has increases the number of possible permutations which increases the length that it takes for someone to "crack" your password using a brute force attack. The table below from the Center for Internet Security shows how the length of a password increases the permutations and time it takes to "crack" the password.

Password Length	Possible Permutations	Time in hours to crack
6	782,757,789,696	0.002
7	75,144,747,810,816	0.21
8	7,213,895,789,838,340	20.04
9	692,533,995,824,480,000	1,923.71
10	66,483,263,599,150,100,000	184,675.73

- The Cybersecurity and Infrastructure Security Agency (CISA) has identified the use of strong passwords as one of the four key actions that organizations and individuals can take to protect themselves online.

- The Federal Trade Commission (FTC), National Institute of Standards and Technology (NIST), and the K12 Security Information eXchange (K12Six) also strongly advocate for the usage of strong passwords.

TECHNICAL DETAILS

Password Policy

- **Staff use a strong password that is 8-24 characters long in addition to Google's 2 Step Verification (2SV).** The initial setup of a strong password and 2SV for new employees will take place during employee onboarding.

- **Students use a strong password that is 8 - 24 characters.** We will not enforce the use of 2SV for students but it is an option if students want to turn it on.

- **Staff and students will be asked to conduct an annual reset of their password.** The date of the reset is determined by Google and set for 365 days since the staff member/student last changed their password.

- **Any active YPICS Google account that has not logged in during the past 45 days will be suspended.** The account will be reactivated once we verify that the user is still a YPICS employee, student, or outside provider. This helps prevent orphaned accounts from being compromised.

What makes a strong password?

We are asking that users create a strong password. To help ensure that passwords are strong, we will be using a setting in the Google Admin console that determines if a password is considered strong.

Google defines a strong password as:

- Has a high level of randomness, called password entropy, which you can achieve using a long string of characters of different types, such as uppercase letters, lowercase letters, numerals, and special characters Note: A strong password doesn't need to have a specific number of characters of a specific type.

- Is not a commonly used weak password, like "123456" or "password123"

- Is not easy to guess, such as simple words or phrases, or patterns in which the password is the same as the username

- Is not known to be compromised—that is, it's not in a database of breached accounts

Reports of suspicious login:

Google will send the tech team a notification if it identifies a login that is outside the user’s normal log in activity. While Google does not explicitly say what is considered a suspicious log in, below are a few reasons we have noticed that this notification is sent.

- **The account is logged in from an IP address outside the normal user’s location.** For example if a user normally logs in from IP addresses in Pacoima but suddenly a login happens from an IP in Boston.

- **Someone successfully logs in from a suspended user’s account.** Since the account is suspended the person who logs in does not access the account but it does mean they have the user's password.

- **The person trying to log in was presented with an extra security question or challenge that they either failed or abandoned.**

When the tech team receives these notifications we will reset the user's password immediately and reset their sign in cookies. Resetting the password will prevent the bad actor from accessing the account. Resetting the user’s sign in cookies will automatically log the account out of any browser or device that the account is logged into. The student will need to reset their password the next time they log in.

REFERENCES

- Center for Internet Security Password Policy Guide
- CISA Creating a Password
- K12 SIX Essential Cybersecurity Protections
- K12 SIX Cybersecurity Standards
- FTC Password Checklist
- Google Support Article on creating strong passwords
- Google Support Article on enforcing and monitoring password requirements for users