You should never store security keys in a version-control system. Cloud Source Repositories can help you prevent users from storing security keys in a Google Cloud repository. Cloud Source Repositories can be set up to check for the following types of security keys:

- Google Cloud service account credentials (JSON format)
- PEM-encoded private keys (including RSA, DSA, and PGP)

This checking feature is available for all repositories at no charge.

When a user executes a `git push` command, the checking feature looks for data that might be a security key. If a match is found, the feature blocks the `git` push and notifies users what was found and where. For example:

To help store security keys more securely, consider using Cloud Key Management Service (/kms/docs/store-secrets).

In the Cloud Console, on the project selector page, select or create a Cloud project.

f you don't plan to keep the resources that you create in this procedure, create a project instead of selecting an existi
t. After you finish these steps, you can delete the project, removing all resources associated with the project.

Go to the project selector page (https://console.cloud.google.com/projectselector2/home/dashboard)

To enable private key detection, use the following `gcloud` command:

To disable security key detection, use the following `gcloud` command:

To override the security key detection feature, use the following `git` command:

After you set up a Google Cloud repository, you might find the following topics helpful:

- Controlling access to repositories (/source-repositories/docs/configure-access-control)
- Using the source browser (/source-repositories/docs/using-source-browser)