Security

🔓 **Personal or network credentials, tokens, server names and more are prohibited from being published to our public repos.** Protect security and credentials with good coding practices. Using local environment files along with `.gitignore` can prevent credentials from being accidentally pushed into your repo. Other guardrails like **pre-commit hooks** can be used to further prevent accidental credential leaks. **See more details on our security policies here**

Listing 1 `local-credentials.yml`

```yaml
# local yaml file that will NOT be pushed to the repo
# add this file to the .gitignore to prevent leaks
my_credentials:
  username: super_secret_user_name
  password: 12345terriblepassword
```

Listing 2 `script-in-repo.R`

```r
# this script is in the repo, but credentials are hidden
library(yaml)

# read in the local credentials yaml file
creds <- yaml::read_yaml("path/to/local_credentials.yml")

# pull in the credentials
username <- creds$my_credentials$username
password <- creds$my_credentials$password
```

Licensing

📄 Each repo in the organization should have a license. Licenses can help prevent your work from being stolen and/or used inappropriately. Licensing details here

Policies

📖 This organization requires each repo to have certain documents, such as a CODE_OF_CONDUCT. The organization uses a special repo called **.github** to ensure all repos adhere to the policies and have the right documents.

Guides

📄 If you're looking to build a repository, check out the Github user guide tabs for best practices on reproducibility, documentation in the repo, and more.