Protect the main branches from direct commits

Avoid unrecognized committers

Define CODEOWNERS for each repository

Separate secret credentials from source code

Avoid committing dependencies into your project

Separate configuration files from source code

Create a meaningful .gitignore file for your projects

Archive dead repositories

Commit early and often

Provide useful commit messages

Add a README.md file to each of your repositories

Add a SECURITY.md file to each of your repositories

Choose an appropriate open source license

Periodically change SSH keys and personal access tokens to mitigate the risk of stolen keys/tokens that you may not even know about

Require two-factor authentication (2FA) for all of your team's GitHub accounts

Remember to revoke repository access when a team member leaves a team or the organization