Add icon Add cover

# GitHub org and repository policies

GitHub provides settings on Enterprise level, where they reflect to all organizations within the enterprise, as well as organization-specific settings. Then, within organizations you create repositories, that have certain settings and policies defined. In this document, the aim is to outline the base settings and policies on all three levels.

## Eneco GitHub organization settings

- Has organization projects = False: we rely on Azure Boards functionality
- Has repository projects = False: we rely on Azure Boards functionality
- Default repository permission = "read": The base permission is that every member can read any repository, but can only contribute based on Team access or specific repository permissions.
- Members can create repositories = True: the aim is that we can only create repositories from code and members can NOT create repositories manually. We are still figuring out what the exact value must be for this specific setting.
- Members can create public repositories = False
- Members can create private repositories = False
- Members can create internal repositories = True
- Members can create pages = False: pages are used to showcase open-source projects or host a blog. If there is a use-case for it, the setting may be reconsidered
- Members can create public pages = False
- Members can create private pages = False
- Members can fork private repositories = False: We don't see a reason to allow this
- Web commit signoff required = True: may not be very relevant in the

Eneco context, but we don't see a reason to disable it

- Advanced security enabled for new repositories = False: this sits behind a paywall and may be covered with Snyk Nel, GF (George) and Strydom, JP (Melanie) please comment with your vision on this
- Dependabot alerts enabled for new repositories = False: **may** sit behind a paywall and may be covered with Snyk Nel, GF (George) and Strydom, JP (Melanie) please comment with your vision on this
- Dependabot security updates enabled for new repositories = False: see above
- Dependency graph enabled for new repositories = False: part of advanced security
- Secret scanning enabled for new repositories = False: part of advanced security
- Secret scanning push protection enabled for new repositories = False: we must test out the behavior

## Templated repository settings and policies

### Repository settings

Enabled:

- Automatically delete head branches
- Always suggest updating pull request branches
- Do not allow bypassing the above settings

Disabled:

All others. Please check any repository in Github to see what options there are

### Branch policies

*Note: policies will only be applied on the main branch*

Enabled:

- Require at least 1 approver, only possible to increase
- Require review from Code Owners

- Require approval of the most recent reviewable push
- Require signed commits
- Dismiss stale reviews

Disabled:

All others. Please check any repository in Github to see what options there are