7. Governance and Policy

Latest updated policy on 10 Apr 2026

---

1. Overview

All GitHub organizations under the Syensqo-SA enterprise are governed by a set of centrally managed organization policies. These policies are automatically applied to ensure consistent security and code quality standards across all teams.

Current Status: Policies are currently running in **Evaluate Mode** -- your actions are not blocked yet, but violations are being recorded. This allows teams to review and adapt before full enforcement is switched on.

---

2. Policies in Effect

There are three categories of policies applied across all repositories in every organization listed above.

2.1 Branch Policies

These rules apply to the **default branch** (e.g., main) of every repository.

Policy	What It Means for You
No branch deletion	The default branch cannot be deleted by anyone
No force pushes	git push --force to the default branch is blocked
Pull Request required	You cannot push directly to the default branch -- all changes must come through a Pull Request
2 approvals required	A PR needs at least **2 approving reviews** before it can be merged
You cannot approve your own last push	If you pushed the most recent commit in a PR, you cannot be one of the approvers
All review threads must be resolved	Every comment thread on the PR must be marked as resolved before the PR can be merged

Example scenarios:

- You open a PR and a reviewer leaves a comment -- the PR cannot be merged until that comment thread is resolved, even if you have 2 approvals.
- You push a commit to your own PR -- you can no longer approve it yourself.
- You try to delete the main branch -- GitHub will block the action.

2.2 Push Policies

These rules are checked **at the time of git push**, before any PR is involved. If your push violates these rules, it will be flagged immediately.

Policy	What It Means for You
Max file path length: 50 characters	File paths (relative to the repo root) longer than 50 characters will be flagged
Blocked file types: .bin, .exe	You cannot push binary executable files into any repository
Max file size: 4 MB	Individual files larger than 4 MB cannot be pushed

Example scenarios:

- You try to push a compiled .exe file -- the push is flagged by the policy.
- You add a large test dataset file of 10 MB -- the push is flagged.
- You create a deeply nested folder like src/components/feature/utils/helpers.js -- the path length will be flagged.

Note: Push policies apply to **every branch**, not just the default branch.

2.3 Tag Policies

These rules protect existing tags across all repositories.

Policy	What It Means for You
No tag deletion	Once a tag is created, it cannot be deleted
No force pushes to tags	You cannot overwrite an existing tag (e.g., moving v1.0.0 to a different commit)

Example scenarios:

- You release 2.0 and want to move the tag to a different commit -- this is blocked.
- You want to remove an old tag like 1.0 -- deletion is blocked.

---

3. Bypass capability for Organization Admins

Organization Admins retain the ability to bypass these rules when necessary:

- **Branch rules** — Admins can bypass via pull request (direct push to default branch is still blocked).
- **Push rules** — Admins can always bypass push restrictions.
- **Tag rules** — Admins can always bypass tag restrictions.

This ensures that in urgent or exceptional situations, your team is not fully blocked. All bypass activity is logged by GitHub for audit purposes, so we recommend using this capability sparingly.

---

4. Where to View Policies in GitHub

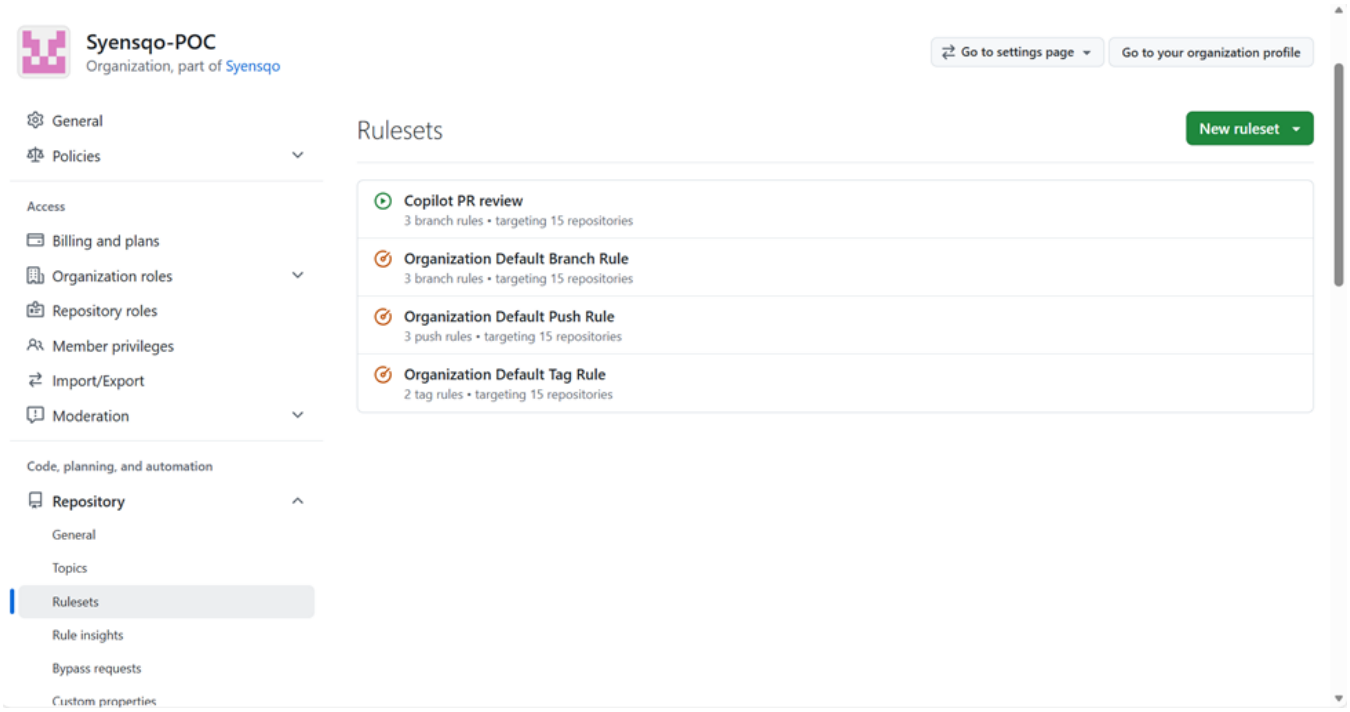
You can view the active rulesets applied to any organization directly in the GitHub UI.

View at the Organization Level

1. Go to your organization on GitHub
2. Click **Settings** (you need at least Maintain access)
3. In the left sidebar, under **Code, Planning and automation**, click **Repository > Rulesets**
4. You will see a list of all rulesets applied to this organization.

Each ruleset entry shows:

- The ruleset name
- The enforcement status (Evaluate / Active)
- Which branches or tags it targets
- The specific rules configured inside it



5. Insights - What Happens When You Are Blocked

Since policies are currently in **Audit (Evaluate) mode**, your pushes and PRs are not hard-blocked yet. However, any violation is recorded and visible in the Rule Insights view.

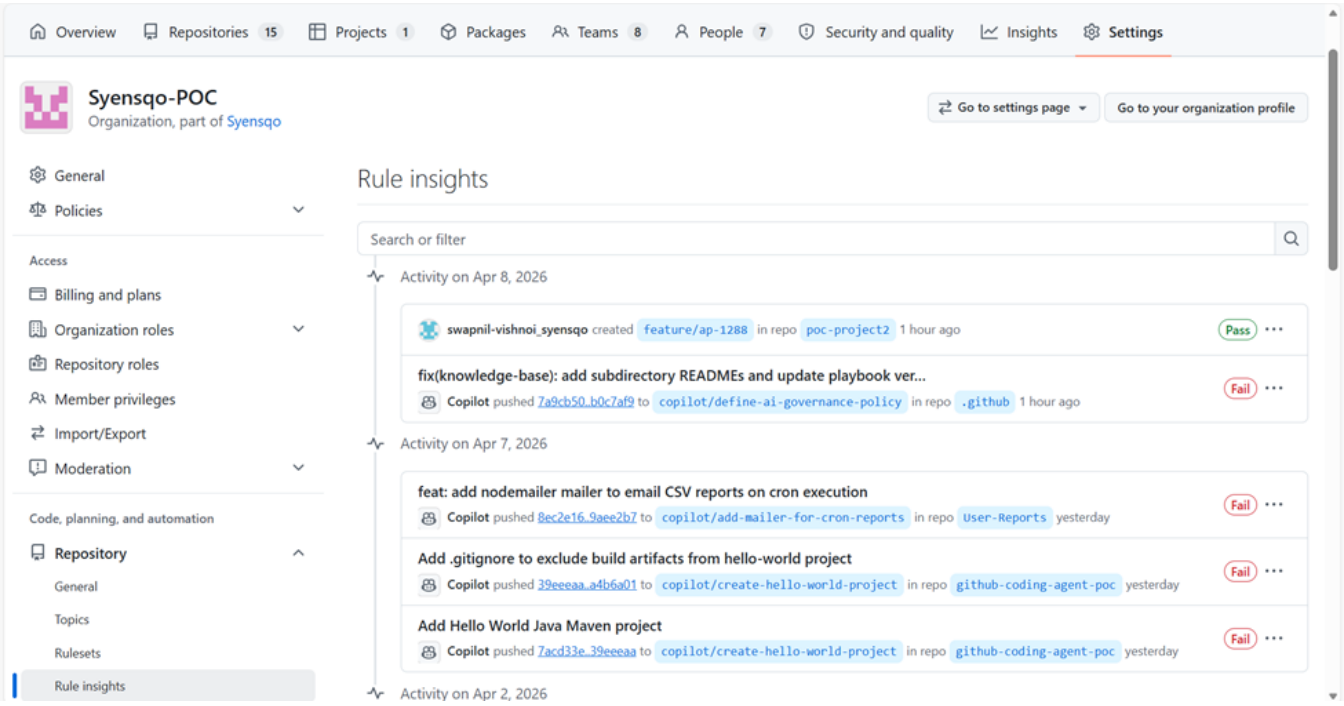
How to Check Rule Insights

1. Go to your organization on GitHub
2. In the left sidebar, under **Code, Planning and automation**, click **Repository > Rule Insights.**

What You Will See

The Rule Insights page shows a log of all recent activity that was evaluated against rulesets:

Column	Description
Ruleset name	Which policy evaluated the action
Actor	The user who triggered the action
Target	The branch, tag, or file that was affected
Result	Pass, Active bypass, Evaluate bypass, or Fail
Timestamp	When the event occurred



If you see **Evaluate bypass** entries against your recent pushes or PRs, that is a signal that your action **will be blocked** once enforcement switches to Active mode. Use this window to fix the issue proactively.