Secrets-Grundsätze

> Zielgruppe: Anwender und Betreuer · Stand: 06.11.2026

Ein Secret, das einmal in einem Log, einem Ticket oder einem Commit stand, gilt als bekannt und muss rotiert werden. Diese Grundsätze verhindern das.

Regeln

- **Nie im Code:** keine Secrets in Repos, `locals`, Default-Werten oder Beispieldateien.
- **Nie in Ausgaben:** Logs, Pipeline-Ausgaben, Tickets, Chats und Doku nennen höchstens den Namen eines Secrets, nie den Wert, auch nicht teilweise.
- **Terraform:** Secrets nicht als Trigger o. Ä. verwenden, die im Plan erscheinen (höchstens als Hash). Werte im State sind unvermeidlich. Deshalb ist der State geschützt.
- **CI-Variablen:** Secrets als masked, hidden und protected anlegen. Protected heißt: nur auf geschützten Branches verfügbar.
- **Skripte:** Trockenlauf als Default. Secrets nur zur Laufzeit lesen (z. B. per stdin), nie als Argument in der Kommandozeile.
- **Neu ablegen:** in OpenBao (siehe Wohin mit Secrets).

> Taucht ein Secret doch in einem Job-Log auf: Fehler beheben, Secret rotieren und danach das Log löschen. In dieser Reihenfolge.

Stolperfallen

- Befehle wie `env`, `printenv` oder `set -x` geben Secrets aus der Umgebung aus.
- Masking in GitLab greift nur bei einzeiligen Werten. Mehrzeilige Werte (z. B. Schlüssel) deshalb Base64-kodiert ablegen.

Weiterführend

- Wohin mit Secrets

Revision #1
Created 2026-11-06 19:02:02 UTC by Alexander Golembek
Updated 2026-11-06 19:02:02 UTC by Alexander Golembek