NAS.AI Security Handbook

Version: 2.0 (Konsolidiert) **Geltungsbereich:** Alle Agenten, Code und Infrastruktur. **Höchste Priorität:** Die Sicherheit des Systems steht über neuen Features.

1. Secrets Management Policy (SMP)

1.1 Die Goldene Regel

NIEMALS echte Secrets (Tokens, Passwörter, Keys) in Code, Dokumentation, Logs oder Git-Commits schreiben.

1.2 Erlaubte Speicherorte

1. **HashiCorp Vault:** Primärer Speicherort (`secret/nas-api/*`).
2. **Environment Variables:** Nur zur Laufzeit injiziert, nicht in `.env` Dateien im Repo.
3. **Password Manager:** Für manuelle Admin-Zugriffe (`/srv/password-manager`).

1.3 Platzhalter

In Dokumentationen sind **IMMER** Platzhalter zu verwenden:

- Vault Token: `hvs.XXXXXXXXXXXXXXXXXXXX`
- API Keys: `re_XXXXXXXXXXXXXXXXXXXXXXXXXX`
- JWT Secrets: `your-secure-secret-here`

1.4 Rotation

Bei Verdacht auf Kompromittierung:

1. Secret sofort revoken.
2. Neu generieren.
3. In Vault/Services aktualisieren.
4. Git-History bereinigen (falls nötig).

2. Security Gates & CI/CD

Deployments werden blockiert, wenn folgende Gates nicht erfüllt sind:

Gate	Bedingung	Prüfer
Gate 1: CVEs	Keine offenen Critical/High CVEs.	PentesterAgent
Gate 2: Tests	Unit-Test Coverage > 80%.	(CI Pipeline)
Gate 3: Secrets	Kein Secret im Code gefunden (Gitleaks/Grep).	Pre-Commit Hook
Gate 4: Auth	Alle Endpoints hinter Middleware Wall (außer `/auth/*`).	APIAgent

Gate 5: CSRF	POST/PUT/DELETE nur mit validem CSRF-Token.	APIAgent

3. Audit Logging Policy

3.1 Was wird geloggt?

- Jeder Login/Logout (Erfolg & Fehler).
- Jede Änderung an Daten (Upload, Delete, Rename).
- Jede Änderung an Berechtigungen oder Systemeinstellungen.
- Paket-Installationen (`package-installs.log`).

3.2 Log-Integrität

- Logs sind **Append-Only**.
- Speicherort: `/var/log/nas-api/audit.log` (und via Loki).
- Format: JSON Structured Logging.

3.3 Incident Response

Bei Erkennung einer Anomalie (z.B. Brute-Force):

1. IP temporär bannen (Fail2Ban).
2. Alert an Orchestrator senden.
3. Incident Ticket erstellen.