node101 Software Dev. Security Policy Summary

01. IAM

2FA and SSH/token usage is mandatory. Permissions must be audited regularly.

02. BRANCH & COMMIT

Signed commits are mandatory. Direct push or force-push is prohibited.

03. CODE REVIEW

At least one approval is required, and approving your own PR is prohibited. Approvals must be reset with new commits, and tests must pass.

04. SECRET YÖNETİMİ

Secrets must never be committed and must be kept in gitignore. In case of leakage, rotation must be immediate, and long-lived secrets must be renewed annually.

05. DEPENDENCY

Lock files must be kept in the repository, and critical vulnerabilities must be patched within 7 days. Dynamic version tags and unmaintained packages are prohibited.

06. CI/CD

Actions must be pinned with commit hashes. Only protected branches can be deployed.

07. APPLICATION SECURITY

Input validation and parameterized queries must be implemented based on OWASP Top 10. Authentication and authorization must be kept separate, and stack traces must be hidden.

08. CRYPTOGRAPHY

Production keys must be protected, and plain text storage is prohibited. Custom cryptography must not be written; standards must be used.

09. INFRASTRUCTURE

Login via SSH key is mandatory, and services must run as non-root. Logs must be kept for 90 days, but they must not contain secrets or personal data.

10. INCIDENT RESPONSE

Report incidents immediately, revoke access, and preserve evidence. Write Post-Mortems within 7 days and respond to SECURITY.md within 72 hours.

APPENDIX: AI USAGE

Confidential data must not be entered into AI tools, and generated code must pass standard security processes.

NODE101 TEKNOLOJİ A.Ş. (Inc.)
Karanfil Sokak, Villa 13 Levent, Beşiktaş, Istanbul /
Turkiye, 34330