vulnerability-testing-policy.md

Vulnerability Testing & Penetration Testing Policy

Purpose

- Define cadence and scope for vulnerability scanning and periodic penetration testing of server-side code and infrastructure.

Scope

- Applies to all server-side repositories, build artifacts, container images, and infrastructure-as-code used in production.

Testing cadence

- Automated dynamic and static scans (SCA for dependencies, SAST for code) run weekly. Results are archived with timestamps.
- Annual or after-major-release penetration test by an internal red team or third-party vendor.

Severity and Remediation

- Critical and High findings must have a remediation ticket created within 24 hours and a coordinated fix deployed within 7 days or documented exception.
- Medium/Low findings: triaged within 7 days, resolved according to release cycles.

Evidence

- We supply: the latest weekly dependency scan JSON and CSV summary, a dated remediation ticket example, and change log entries showing a vulnerability fix reference.

Process

- Scanning: use npm audit / SCA toolchain during CI, store raw JSON to evidence storage with a timestamp and commit hash.
- Triage: security owner tags severity and assigns to an owner who creates a JIRA/GH issue (sample ticket included).

Review cadence

- Weekly automated runs with a weekly digest emailed to security and dev leads.

Contact

- security@autopromote.example