code-backend-updates-policy.md

Code & Backend Updates / Patch Management Policy

Purpose

Describe how we maintain 3rd-party dependencies, scan for vulnerabilities, and apply patches in a repeatable way.

Scope

All third-party libraries, SDKs, and frameworks used in server-side components.

Process

1. Identification
   - Automated dependency scans run weekly (e.g., `npm audit`, Snyk, other SCA tools). Findings are recorded.
2. Prioritization
   - Prioritize by severity (CVSS) and exploitability. Critical/high vulnerabilities are triaged immediately.
3. Remediation
   - For each vulnerable dependency: update to a patched version, run unit/integration tests, and deploy to staging.
   - If no patch exists, implement compensating controls or version pinning and document risk acceptance.
4. Verification
   - After patch, re-run the dependency scan to verify remediation.
5. Communication
   - Track actions in the ticketing system and notify stakeholders of high-severity issues.

Evidence and artifacts for reviewers

- Provide a dependency scan output (for example, `npm audit --json` or Snyk report) that includes:
  - Date of the scan (must be within 12 months of the assessment notification)
  - Summary of high/critical vulnerabilities and their status
  - Testing methodology or commands used (e.g. `npm audit --json`, `snyk test --json`)

Responsibilities

- Engineering: run scans, fix issues and deploy patches
- Security Owner: validate critical fixes and sign off