 # Secure Development Checklist (v1)

***Context:** Early-stage static site; checklist prepared for future interactive features.

1. Authentication & Sessions
- Use proven auth libraries (avoid rolling your own).
- Store passwords with bcrypt/argon2 (cost ≥12).
- Enforce Secure, HttpOnly, SameSite=strict cookies or use short-lived JWTs + refresh tokens with rotation.
- Implement account lockout + rate limit for auth endpoints.

2. Authorization & Access Control
- Enforce server-side ownership checks for every object (IDOR prevention).
- Use non-predictable identifiers (UUIDs) where appropriate.
- Principle of least privilege for admin functions.

3. Input Validation & Output Encoding
- Validate and sanitize all inputs server-side (whitelists).
- Use contextual output encoding (HTML, JS, URL).
- Prevent reflected & stored XSS via proper escaping and CSP headers.

4. File Uploads & Exports
- Validate file type and size server-side.
- Store uploads outside webroot; serve via signed URLs with short TTL.
- Scan uploaded files for malware if possible.

5. API & CORS
- Restrict CORS to allowed origins for sensitive endpoints.
- Do not use Access-Control-Allow-Origin: * for endpoints returning user-specific data.
- Enforce proper auth on all API endpoints.

6. Secrets & Configuration
- Do not hardcode secrets in JS or repos; use environment variables and secret manager.
- Ensure no API keys or credentials in client-side bundles.

7. Logging, Monitoring & Response
- Log auth failures, export downloads, and admin actions.
- Monitor anomalous access patterns; configure alerts for spikes.
- Maintain a simple incident response playbook.

8. Deployment & CDN
- Use HTTPS everywhere (HSTS), set secure headers: CSP, X-Frame-Options, X-Content-Type-Options, Referrer-Policy.
- Configure WAF rules for common web attacks if using public hosting.

9. Developer Hygiene
- Use code review for security-sensitive changes.
- Run dependency vulnerability scans (Dependabot/OSS scanners).
- Keep third-party libs up to date.

10. Pre-launch checklist
- Authentication stress test, role-based access checks, file upload tests, export/privilege tests, and a final security review before public interactive launch.