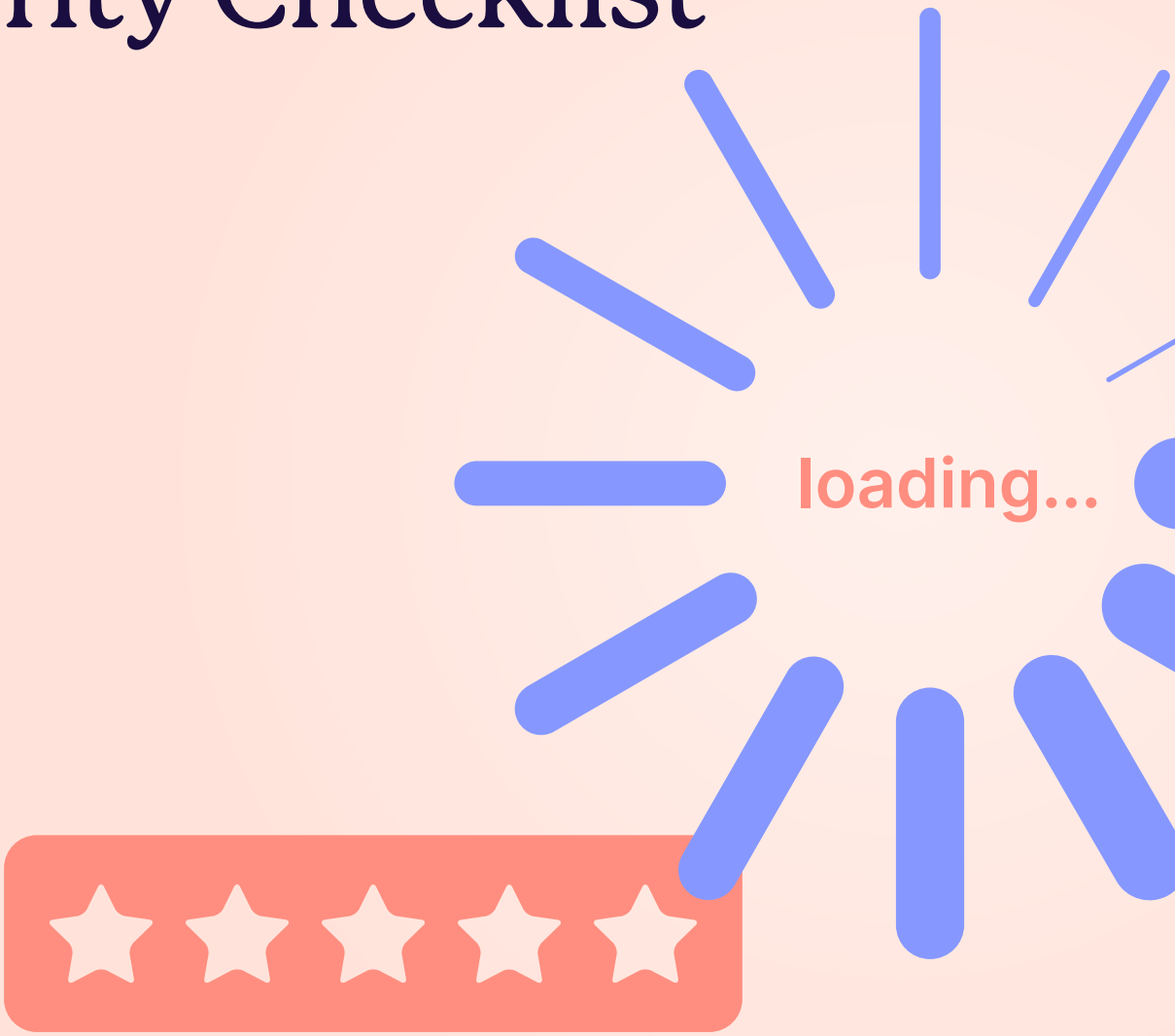
greenhat

Website Performance and Security Checklist



Follow us on LinkedIn to receive more powerful IT checklists for your business.

CHECKLIST

Cadence _____

Last Review _____

Date _____

By _____

Website Performance and Security Checklist

Website performance and security are two intertwined pillars crucial for your online presence. A fast-loading, responsive site builds trust and ensures user satisfaction; while robust security measures protect your business assets and user data. This checklist will help ensure that your website meets the highest standards in both performance and security.

- [ ] Site Load Speed
  - [ ] Website (mobile & desktop) load speed is within target range (use Google PageSpeed Insights).
  - [ ] Website is free of serious performance inhibitors.
- [ ] SSL/TLS Certificate
  - [ ] Website uses HTTPS for secure communication.
  - [ ] Certificate is valid (i.e., no “not secure” browser warnings).
- [ ] Content Delivery Network (CDN) Integration
  - [ ] Using a CDN to distribute website content to reduce latency and improve site load times.
- [ ] Mobile Optimization
  - [ ] Website is responsive and user-friendly on mobile devices.
  - [ ] Mobile load times is within target range.
  - [ ] Site user experience is consistent across various screen sizes.
- [ ] Regular Backups
  - [ ] Are regularly backing up website based on a schedule.
  - [ ] Backups are stored securely, and the restoration process is periodically tested.
- [ ] Distributed Denial of Service (DDoS) Protection
  - [ ] Have measures to detect and mitigate Distributed Denial of Service attacks.
- [ ] Code, CMS & Plugin Updates
  - [ ] Code base is up to date.
  - [ ] All Content Management System (e.g., WordPress, Joomla) versions plugins/extensions are up to date.
- [ ] Online Forms Functional & Secure
  - [ ] All online forms (including integrations) are functioning as intended.
  - [ ] Online forms have bot prevention (like reCAPTCHA) & function properly.
- [ ] User Access & Permissions
  - [ ] Using strong passwords and two-factor authentication for all logins.
  - [ ] User permissions regularly audited, with only necessary permissions granted.
- [ ] Security Audits
  - [ ] We have a regular cadence of security audits scheduled.
  - [ ] We regularly scan for malware or suspicious activities.