

WEBFORLESS · SINCE 2003

Website Maintenance Calendar

A launch is the beginning of website ownership, not the end of the project. Maintenance protects security, performance, content accuracy, accessibility and business continuity as browsers, devices, dependencies and customer expectations change.

Use this guide to:	Clarify priorities, assign ownership, identify risk and verify implementation.
Website:	webforless.ca

Project / website: _____

Owner: _____ Review date: _____

1. Maintenance is risk management

A neglected website may continue to look normal while dependencies age, backups fail, forms stop delivering or information becomes inaccurate. Maintenance creates a routine for finding small problems before they become expensive incidents.

- | |
|---|
| ■ Assign owners for technical and content tasks. |
| ■ Record maintenance work and unresolved risks. |
| ■ Match review frequency to business importance and change. |

Notes / evidence:

2. Updates require staging and verification

Software updates can fix vulnerabilities and compatibility issues, but blind updating can also break templates or integrations. A controlled process reviews changes, backs up the site, tests in staging and verifies the production release.

- | |
|---|
| ■ Review release notes and dependencies. |
| ■ Test forms, payments and critical journeys. |
| ■ Keep a rollback path for important changes. |

Notes / evidence:

3. Backups are only useful when they restore

A backup plan specifies what is copied, how often, where copies are stored, how long they are retained and who can restore them. At least one copy should be isolated from the production environment. Restoration tests are essential.

- | |
|--|
| ■ Back up files, databases and configuration. |
| ■ Encrypt and restrict backup access. |
| ■ Practice restoration and document recovery time. |

Notes / evidence:

4. Security needs continuous attention

Maintenance includes vulnerability review, access control, certificate renewal, log monitoring, malware detection and removal of unused accounts or plugins. Security should reduce exposure without creating unnecessary friction for legitimate users.

- | |
|---|
| ■ Use unique accounts and multifactor authentication. |
| ■ Remove abandoned components. |
| ■ Create an incident response contact path. |

Notes / evidence:

5. Content and accessibility also decay

Hours, prices, team details, policies and links change. New content may introduce inaccessible headings, images, forms or colour combinations. Maintenance should review accuracy and usability, not only software versions.

- | |
|---|
| ■ Schedule content ownership reviews. |
| ■ Check broken links and outdated claims. |
| ■ Include accessibility checks in publishing workflows. |

Notes / evidence:

6. Performance must be watched over time

New analytics tags, chat widgets, fonts and media gradually increase page weight. Real-user monitoring, page-weight budgets and periodic audits help prevent slow decline.

- | |
|---|
| ■ Review third-party scripts. |
| ■ Compress and resize new media. |
| ■ Monitor key templates and conversion pages. |

Notes / evidence:

7. Use a practical maintenance rhythm

Daily automation can monitor uptime and errors. Monthly work can review updates, forms and security. Quarterly reviews can assess content, accessibility and performance. Annual planning can revisit architecture, hosting and disaster recovery.

- | |
|---|
| ■ Automate alerts but assign human ownership. |
| ■ Prioritize business-critical pages. |
| ■ Use the calendar as a minimum, not a rigid ceiling. |

Notes / evidence:

Launch and follow-up review

Item	Owner	Status / date
Critical journey tested		
Access and ownership documented		
Backups or rollback verified		
Analytics and monitoring confirmed		
Outstanding risks recorded		
30-day review scheduled		

Good websites and software are never finished. They are monitored, maintained and improved as evidence and needs change.