DBS Interactive Maintenance Plan

A new site launches healthy. It does not stay that way on its own. Standards, threats, and best practices keep changing. The DBS Site Maintenance and Security plan keeps your site aligned with them, on a schedule and the day an urgent fix ships.

WHAT THE PLAN COVERS

- CMS (Craft) updates twice per year, plus critical updates within one business day
- Site speed monitoring and adjustments
- Continued adherence to Google's best practices
- Functionality adjustments as best practices change (e.g., PWA standards for search engines)
- Ongoing alignment with site-specific compliance standards (e.g., GDPR)
- Website security maintenance, including updates for unused software components on the server
- PWA (Progressive Web App) maintenance
- Accessibility testing and remediation to current standards
- Browser compatibility updates
- Monthly Site Health Report and scorecard

CMS Updates & Website Security

Regular updates protect your site from security threats and keep it current with the latest technology. DBS updates your CMS two times per year. Without a maintenance plan, these upgrades carry an additional charge. DBS installs critical updates within one business day.

Critical Updates

Critical Updates are updates DBS applies with priority to protect site security, availability, data integrity, or legal and compliance posture.

> **When an update counts as Critical:** the vendor labels the issue Critical or High, or the CVE or NVD CVSS base score is 7.0 or higher.

Vulnerability Updates

A vulnerability is a flaw, weakness, or misconfiguration in software that an attacker could exploit to compromise the confidentiality, integrity, or availability of a system or its data. Common classes include:

Remote Code Execution (RCE)
Attacker gains the ability to run arbitrary code

Code & Template Injection
Malicious code inserted into the application

SQL Injection
Attacker manipulates database queries

Cross-Site Scripting (XSS)
Malicious scripts run in visitors' browsers

Cross-Site Request Forgery (CSRF)
Unauthorized actions sent as a trusted user

Privilege Escalation
Attacker gains more permissions than intended

Information Disclosure
Sensitive data leaks

Authentication Bypass
Access controls get circumvented

Directory Traversal & File Inclusion
Attacker reaches files outside intended paths

And more
The list grows as new threats emerge

Site Performance

Site performance matters to your visitors and to Google. Browser, device, and search engine standards keep evolving. DBS makes sure your site evolves with them. DBS measures four factors:

Google Best Practices | **PWA** | **Digital Accessibility** | **Speed**

Digital Accessibility Compliance

DBS runs automated accessibility tests on a regular schedule. Accessibility gives every visitor, including people living with disabilities, full access to your site. It also supports legal compliance and meets Google's best practice requirements.

Automated tools alone cannot guarantee compliance. DBS recommends an annual manual audit, quoted separately based on your needs.

Browser Compatibility & Other Compliance

A DBS-built site launches compliant with the agreed-upon browsers. The web keeps changing, so the site needs updates to protect the integrity of its design and user experience.

- DBS can monitor your site for changes to other compliance standards once implemented, such as GDPR (General Data Protection Regulation).
- DBS bases these updates on user traffic data to deliver a consistent, quality experience for your visitors.

Keep your site ready for the next advisory
Talk with DBS Interactive about a maintenance plan for your website.

dbswebsite.com