

Maintenance WordPress Que doit contenir un vrai contrat de maintenance ?

Un contrat de maintenance WordPress ne devrait pas se limiter à faire les mises à jour. Il doit préciser le périmètre, les sauvegardes, les tests, la sécurité, les délais d'intervention, les responsabilités, les accès, le reporting et les limites de prise en charge.

Publié le 26 juin 2026

Ce document reproduit le contenu publié à l'adresse indiquée en pied de page, dans sa version disponible à la date de sa génération. Il est fourni à titre exclusivement informatif et ne constitue ni un conseil juridique, réglementaire, fiscal ou professionnel, ni une garantie d'exhaustivité, d'exactitude ou d'actualité. Les textes officiels et la situation propre du lecteur doivent être vérifiés avant toute décision. Dans les limites permises par la loi applicable, Nasteo n'assume aucune responsabilité au titre des décisions prises ou des conséquences résultant de l'utilisation de ce document.

Un contrat utile dit clairement ce qui est maintenu, testé, surveillé et exclu

Un vrai contrat de maintenance WordPress doit répondre à une question simple : que se passe-t-il quand le site doit être mis à jour, surveillé, restauré ou réparé ?

Beaucoup de contrats se contentent de formules vagues : “maintenance du site”, “mises à jour incluses”, “sécurité”, “support technique”. Pour une PME, ces formulations sont insuffisantes. Elles ne disent pas ce qui est réellement fait, à quelle fréquence, avec quelles sauvegardes, dans quels délais, par qui, ni avec quelles limites.

Le point critique est de ne pas confondre maintenance préventive, maintenance corrective, maintenance sécurité, maintenance évolutive et infogérance d’hébergement. Un contrat peut inclure certaines de ces dimensions, mais rarement toutes sans limites.

Le bon objectif n’est pas d’obtenir une promesse de “tout compris”, mais un document qui clarifie le périmètre, les exclusions, les accès, les sauvegardes, les délais, les responsabilités, les licences, la sortie de contrat et les obligations RGPD lorsque le prestataire accède à des données personnelles.

“Maintenance WordPress” : une expression trop vague

Pour un dirigeant de PME, la maintenance WordPress ressemble souvent à une ligne de facture mensuelle. Tant que le site fonctionne, le sujet paraît secondaire. Mais dès qu’un formulaire ne part plus, qu’une mise à jour casse la mise en page, qu’un plugin devient vulnérable ou qu’un site est infecté, la question revient immédiatement : que comprend exactement notre contrat ?

C’est là que les malentendus apparaissent. Le client pense parfois que le prestataire “s’occupe de tout”. Le prestataire, lui, considère souvent que son contrat couvre les mises à jour de base et une surveillance limitée. Entre les deux, il peut manquer des éléments essentiels : restauration, nettoyage après piratage, correction WooCommerce, problème d’email, intervention hors horaires, conflit entre plugins, optimisation de performance, support Elementor, gestion DNS ou assistance hébergeur.

Un bon contrat de maintenance n’a pas pour but de tout promettre. Il sert à clarifier le périmètre, les responsabilités et les délais. Il doit permettre à l’entreprise de savoir ce qui est inclus, ce qui ne l’est pas, ce qui relève d’une intervention exceptionnelle, et ce qui doit être traité par un autre prestataire.

Les quatre familles de maintenance à distinguer

Toutes les maintenances ne couvrent pas le même besoin. Le contrat doit dire clairement de quoi il parle.

Type de maintenance Objectif Exemples
Maintenance préventive Éviter les problèmes Mises à jour, sauvegardes, contrôles réguliers, surveillance.
Maintenance corrective Corriger un dysfonctionnement Bug formulaire, erreur PHP, conflit plugin, page cassée.
Maintenance sécurité Réduire les risques et réagir aux alertes Correctifs de sécurité, durcissement, analyse malware, gestion des accès.

Maintenance évolutive | Faire évoluer le site | Nouvelle page, nouveau bloc, fonctionnalité, optimisation UX.

Point de vigilance Une maintenance préventive peut inclure les mises à jour, mais pas forcément la correction complète d'un conflit complexe. Une maintenance sécurité peut inclure la surveillance, mais pas nécessairement le nettoyage d'un site déjà compromis avant le contrat.

Le périmètre technique : ce qui doit être listé

Un contrat sérieux doit commencer par une cartographie du site. Cette cartographie évite une situation fréquente : un incident survient sur un élément que personne ne pensait être "dans le contrat".

Élément À préciser dans le contrat
WordPress core Version suivie, mises à jour mineures/majeures, stratégie de test.
Thème actif Thème parent, thème enfant, constructeur utilisé, personnalisations.
Extensions Liste des plugins critiques, plugins premium, licences, extensions abandonnées.
WooCommerce Commandes, paiement, emails, compatibilités, tests spécifiques.
Elementor ou builder Modèles, CSS générés, widgets, dépendances.
Hébergement Inclus ou non, accès serveur, PHP, base de données, logs.
Domaine / DNS Inclus ou exclu, accès registrar, Cloudflare éventuel.
Emails transactionnels SMTP, formulaires, WooCommerce, délivrabilité minimale.
Sauvegardes Fréquence, rétention, stockage, test de restauration.
Sécurité Surveillance, scans, alertes, durcissement, logs.
Performance Cache, poids des pages, images, erreurs, Core Web Vitals éventuels.

Les mises à jour : nécessaires, mais jamais automatiques à l'aveugle

La maintenance WordPress est souvent réduite aux mises à jour. C'est une erreur. Mettre à jour est indispensable, mais une mise à jour peut créer un conflit : extension incompatible, thème non maintenu, version PHP trop ancienne, changement WooCommerce, widget Elementor modifié, conflit JavaScript, panier cassé.

WordPress recommande de sauvegarder le site avant une mise à niveau, et sa documentation rappelle qu'un site WordPress typique nécessite à la fois les fichiers et la base de données pour être restauré correctement.

Préproduction / staging

Un site de préproduction, ou staging, est une copie du site utilisée pour tester les mises à jour avant de les appliquer sur le site public. Pour un site simple, ce n'est pas toujours indispensable. Pour un WooCommerce, un site Elementor complexe ou un site à fort enjeu commercial, c'est souvent une sécurité importante.

Sujet Question à clarifier
Fréquence Mises à jour hebdomadaires, mensuelles, urgentes ?
Typologie Core WordPress, thèmes, plugins, extensions premium ?
Sécurité Correctifs urgents traités plus vite que les mises à jour fonctionnelles ?
Test avant mise à jour Préproduction, sauvegarde, contrôle visuel, test critique ?
Retour arrière Qui restaure si la mise à jour casse le site ?
Extensions abandonnées Qui alerte et propose une alternative ?
WooCommerce Test du panier, du paiement et des emails de commande ?
Elementor Vérification des modèles et pages clés ?

Le contrat doit aller au-delà de “sauvegarde incluse”

Une ligne “sauvegarde incluse” ne suffit pas. Le contrat doit préciser ce qui est sauvegardé, où, combien de temps, avec quel niveau d'isolation, et quand la restauration a été testée.

Question Pourquoi c'est important
Que sauvegarde-t-on ? Fichiers, base, médias, configuration, tables plugins.
À quelle fréquence ? Le besoin diffère entre site vitrine et e-commerce.
Où sont stockées les copies ? Même serveur, espace distant, coffre isolé.
Combien de versions sont conservées ? Revenir avant une attaque ancienne peut être nécessaire.
Qui peut restaurer ? Éviter la dépendance à une seule personne.
Quand la restauration a-t-elle été testée ? Une sauvegarde non testée reste théorique.
Quel délai de restauration est prévu ? Continuité commerciale et urgence client.
Que se passe-t-il après piratage ? Restaurer sans diagnostic peut réinstaller la faille.

Surveillance, prévention et limites

Un contrat de maintenance ne transforme pas un site vulnérable en forteresse. Il doit en revanche prévoir un socle de sécurité raisonnable : accès, scans, alertes, corrections, durcissement et limites de prise en charge.

Mesure À préciser
Comptes administrateurs Nombre, personnes autorisées, suppression des anciens accès.
Authentification forte 2FA pour les comptes sensibles.
Mots de passe Politique, renouvellement après incident.
Extensions vulnérables Veille, alerte, correction ou remplacement.
Scan de sécurité Fréquence, outil, périmètre.
Logs Conservation, consultation, limites hébergeur.
Fichiers sensibles Droits, désactivation de l'édition de fichiers, protection des uploads.
Pare-feu applicatif Inclus ou non, plugin ou solution externe.
Nettoyage malware Inclus, exclu ou facturé à part.
Durcissement serveur Inclus seulement si l'hébergement est dans le périmètre.

Ne pas confondre surveillance et garantie absolueLa documentation WordPress sur le durcissement couvre plusieurs familles de mesures, serveur, base, permissions, configuration, plugins, thèmes, accès, mais aucune mesure isolée ne suffit. Le contrat doit dire ce qui est réellement fait et ce qui reste hors périmètre.

Ce qu'il faut écrire noir sur blanc

Le contrat doit distinguer délai de prise en compte et délai de résolution. Un prestataire peut s'engager à prendre en charge une demande sous quatre heures ouvrées, sans pouvoir garantir que le problème sera résolu dans ce délai.

Niveau Exemple Engagement possible
Critique Site indisponible, paiement impossible, piratage visible. Prise en compte prioritaire.
Important Formulaire cassé, erreur sur page clé, email transactionnel bloqué. Traitement sous délai contractuel.
Standard Correction mineure, ajustement visuel, question technique. Traitement planifié.
Évolutif Nouvelle fonctionnalité, nouvelle page, refonte partielle. Devis ou forfait séparé.

Les horaires doivent être explicites : jours ouvrés, heures ouvrées, astreinte, week-end, jours fériés. Sans astreinte écrite, il ne faut pas supposer qu'une intervention urgente le dimanche soir est incluse.

Ce qui est souvent exclu, mais rarement compris

Un bon contrat doit aussi dire ce qui n'est pas inclus. Ces exclusions ne sont pas négatives : elles évitent les malentendus et permettent de chiffrer correctement les interventions exceptionnelles.

Sujet souvent exclu Pourquoi
Refonte graphique Relève d'un projet distinct.
Développement sur mesure Demande cadrage, test et recette.
Ajout de fonctionnalités Impact technique et maintenance future.
Nettoyage d'un site déjà infecté Intervention de crise, souvent hors forfait.
Correction d'un plugin tiers abandonné Le prestataire ne contrôle pas son code.
Hébergement externe Limites d'accès et de responsabilité.
Problèmes DNS ou domaine Parfois gérés par un autre acteur.
Délivrabilité email Dépend de DNS, SMTP, réputation et outils tiers.
SEO éditorial Différent de la maintenance technique.
Conformité RGPD complète Sujet juridique, organisationnel et technique.

Un point stratégique pour l'entreprise

La maintenance WordPress touche à des accès sensibles. L'entreprise doit savoir qui possède quoi. Le prestataire peut gérer techniquement, mais l'entreprise doit conserver la maîtrise de ses actifs essentiels : domaine, hébergement, sauvegardes, comptes stratégiques et licences dont elle dépend.

Accès Question à poser
WordPress administrateur L'entreprise a-t-elle un compte administrateur propre ?
Hébergement L'entreprise peut-elle ouvrir un ticket ou restaurer ?
Nom de domaine Le domaine est-il bien au nom de l'entreprise ?
DNS Qui peut modifier les entrées critiques ?
Licences premium Appartiennent-elles au client ou au prestataire ?
Sauvegardes L'entreprise peut-elle en obtenir une copie ?
Analytics / Search Console Qui en est propriétaire ?
SMTP / emailing Qui détient les accès ?

Licences agence ou développeur

Beaucoup de prestataires utilisent des licences “agence”, “développeur” ou multisites pour Elementor Pro, des plugins de sécurité, de sauvegarde, de SEO ou de formulaires. Ce modèle peut être normal, mais il doit être clair. Si la licence appartient au prestataire, le client doit savoir ce qui se passe à la fin du contrat : maintien temporaire, transfert vers une licence client, remplacement de l’outil, ou perte des mises à jour premium.

Prestataire, sous-traitance et accord de traitement des données

Un prestataire qui maintient un site peut accéder à des données personnelles : formulaires de contact, comptes utilisateurs, commandes WooCommerce, logs, adresses email, demandes de devis ou exports.

Article 28 du RGPD Dès lors qu’un prestataire de maintenance accède à des données personnelles, il agit généralement comme sous-traitant au sens du RGPD. L’article 28 impose alors un contrat écrit entre l’entreprise et le prestataire, souvent appelé accord de traitement des données ou DPA. Ce n’est pas une simple bonne pratique : c’est une obligation légale.

Ce contrat écrit doit préciser notamment l’objet, la durée, la nature des traitements, les catégories de données, les obligations de confidentialité, les mesures de sécurité, l’assistance, les sous-traitants ultérieurs et le sort des données en fin de contrat. Pour une PME, il ne s’agit pas de transformer le contrat de maintenance en traité juridique illisible, mais les accès aux données et les responsabilités doivent être cadrés.

Reporting : la preuve que la maintenance existe

Une maintenance invisible peut être réelle. Mais pour un dirigeant, elle doit être compréhensible. Le reporting permet de répondre à trois questions : qu’a-t-on fait ? qu’a-t-on détecté ? que faut-il décider ?

Élément Exemple
Mises à jour réalisées WordPress, thème, plugins.
Sauvegardes Date, statut, rétention, incident éventuel.
Sécurité Alertes, comptes suspects, vulnérabilités traitées.
Disponibilité Incidents constatés, temps d’arrêt.
Performance Anomalies, cache, erreurs récurrentes.
Actions correctives Bugs corrigés, interventions.
Points de vigilance Plugin à remplacer, PHP à migrer, licence expirée.
Recommandations Actions à prévoir, risques à arbitrer.

Maintenance WordPress et hébergement : deux périmètres à ne pas confondre

La maintenance WordPress porte sur le site. L'hébergement porte sur l'environnement qui permet au site de fonctionner : serveur, PHP, base de données, espace disque, sauvegardes serveur, certificats SSL, logs, sécurité système, disponibilité. Parfois, le même prestataire gère les deux. Parfois non.

Sujet Maintenance WordPress Hébergement / infogérance
Mises à jour plugins Oui Non, sauf contrat global.
Version PHP Suivi et alerte Modification serveur.
Espace disque Alerte éventuelle Gestion serveur.
Sauvegarde fichiers/base Selon contrat Selon offre hébergement.
Pare-feu serveur Rarement Oui si infogérance.
Logs serveur Consultation limitée Accès complet.
Certificat SSL Parfois Souvent hébergement.
Sécurité OS Non Oui si serveur managé.

Un niveau de maintenance plus exigeant

Un site WooCommerce n'est pas un simple site vitrine. Il porte des commandes, des paiements, des clients, des stocks, des emails transactionnels et parfois des obligations comptables. Sans tests spécifiques, une mise à jour peut sembler réussie alors que le site ne vend plus correctement.

Élément WooCommerce Test attendu
Panier Ajout, suppression, modification quantité.
Tunnel de commande Validation complète jusqu'au paiement test.
Paiement Stripe, PayPal, banque, 3DS éventuel.
Emails Commande client, notification admin, facture.
Stocks Décrémentations, rupture, variation.
Comptes clients Création, connexion, mot de passe oublié.
Taxes / livraison Règles principales vérifiées.
Extensions WooCommerce Abonnements, factures, transporteurs, exports.

Les zones grises qui créent les litiges

Erreur Conséquence
"Mises à jour incluses" sans détail Impossible de savoir ce qui est réellement couvert.
Aucun test après mise à jour Bug détecté par les clients.
Pas de sauvegarde avant intervention Retour arrière difficile.
Pas de délai de prise en compte Urgence mal gérée.
Pas de distinction correctif / évolutif Conflit sur les demandes client.
Pas de reporting Maintenance invisible et difficile à évaluer.
Accès détenus uniquement par le prestataire Dépendance dangereuse.
Pas de clause RGPD Accès aux données mal encadré.
WooCommerce traité comme un site vitrine Risque commercial direct.
Nettoyage piratage non cadré Coût imprévu, délai de reprise inconnu et possible blocage opérationnel en pleine crise.
Pas de sortie de contrat Récupération difficile des accès et sauvegardes.

Que demander avant de signer ?

Question Si la réponse est floue
Quelles mises à jour sont incluses ? Vous ne savez pas ce qui est réellement maintenu.
Une sauvegarde est-elle faite avant intervention ? Une mise à jour peut devenir risquée.
Les restaurations sont-elles testées ? Les sauvegardes restent théoriques.
Quels délais sont prévus selon la gravité ? Une urgence peut attendre trop longtemps.
Le contrat couvre-t-il WooCommerce ? Le tunnel de vente peut être mal protégé.
Le nettoyage après piratage est-il inclus ? Le coût et le délai de reprise peuvent être inconnus en crise.
Le prestataire dispose-t-il d'une RC Pro adaptée ? En cas d'erreur, d'indisponibilité ou de dommage lié à l'intervention, les recours peuvent être limités.
Qui possède les licences premium ? Dépendance ou rupture à la fin du contrat.
Qui détient le domaine et l'hébergement ? Risque de blocage opérationnel.
Recevez-vous un reporting ? Impossible d'évaluer la prestation.

Ce que devrait contenir un contrat utile

1 Périmètre et responsabilités

Identité du site, éléments maintenus, fréquence des contrôles, stratégie de mise à jour, exclusions, délais et horaires.

2 Sauvegardes et sécurité

Sauvegardes, tests de restauration, surveillance, gestion des vulnérabilités, traitement des incidents et limites de garantie.

3 Accès, licences et RGPD

Accès nécessaires, propriété des licences, accord de traitement des données si accès à des données personnelles.

4 Sortie et restitution

Conditions de sortie et de restitution : accès, sauvegardes, licences, documentation, comptes tiers et état technique du site.

Ce que les lecteurs demandent souvent

Une maintenance WordPress mensuelle est-elle indispensable ?

Elle est fortement recommandée pour un site professionnel, surtout si le site utilise plusieurs extensions, un constructeur comme Elementor, WooCommerce, des formulaires ou des fonctionnalités critiques. Un site peu maintenu peut rester en ligne, mais il devient progressivement plus fragile.

Les mises à jour automatiques suffisent-elles ?

Pas toujours. Par défaut, WordPress applique automatiquement certaines mises à jour mineures du cœur, notamment les correctifs de maintenance et de sécurité. Les mises à jour majeures, les extensions et les thèmes ne sont pas nécessairement mis à jour automatiquement, sauf activation explicite ou configuration spécifique. Même lorsqu'elles sont activées, les mises à jour automatiques ne remplacent pas une sauvegarde, un contrôle visuel, un test des fonctions critiques et une procédure de retour arrière.

Faut-il tout mettre à jour dès qu'une version sort ?

Non. Les correctifs de sécurité doivent être traités rapidement. Les mises à jour fonctionnelles peuvent parfois être testées avant déploiement, surtout sur un site complexe.

Un contrat de maintenance doit-il inclure le nettoyage après piratage ?

Il peut l'inclure, mais ce n'est pas automatique. Beaucoup de contrats prévoient la surveillance et les correctifs, mais facturent séparément le nettoyage d'un site compromis, surtout si l'infection est antérieure au contrat. Le point doit être écrit pour éviter un coût imprévu et un délai de reprise inconnu en pleine crise.

Le prestataire doit-il avoir un compte administrateur ?

Oui, s'il intervient techniquement. Mais l'entreprise doit aussi conserver un accès administrateur propre, sécurisé, documenté, et éviter que tout repose sur le compte du prestataire.

La maintenance inclut-elle le SEO ?

La maintenance technique peut protéger certains éléments SEO : disponibilité, erreurs, redirections, performance, indexation, sécurité. Mais la stratégie SEO, les contenus, le netlinking ou l'optimisation éditoriale relèvent généralement d'une prestation séparée.

Qui doit payer les licences premium ?

Les deux modèles existent. Si les licences sont celles du prestataire, il faut savoir ce qui se passe à la fin du contrat. Si elles appartiennent au client, il faut prévoir leur renouvellement et leur gestion. Le cas des licences "agence" doit être explicite.

Le contrat doit-il prévoir une sortie ?

Oui. C'est un point essentiel. Le client doit pouvoir récupérer les accès, sauvegardes, licences dont il est propriétaire, documentation utile, comptes tiers et état technique du site.

Un bon contrat protège autant la PME que le prestataire

Un vrai contrat de maintenance WordPress ne se résume pas à une promesse de mises à jour. Il clarifie ce qui est fait, ce qui est surveillé, ce qui est testé, ce qui est exclu, qui décide, qui intervient, dans quels délais, et avec quels accès.

Pour une PME, cette clarté évite deux risques : payer une prestation trop vague, ou découvrir en crise que le sujet critique n'était pas couvert.

Le bon contrat n'est pas forcément le plus long. C'est celui qui permet de répondre simplement : notre site est-il suivi, sauvegardé, sécurisé, testable, restaurable, et savons-nous quoi attendre de notre prestataire ?

Sources

- WordPress.org, Backups / Advanced Administration Handbook : sauvegardes régulières, sauvegarde avant mise à jour, fichiers et base de données nécessaires à la restauration.
- WordPress.org, Hardening WordPress : durcissement, sécurité serveur, permissions, configuration, plugins, thèmes et accès.
- WordPress.org, Upgrading WordPress : sauvegarde avant mise à niveau, processus de mise à jour, configuration des mises à jour automatiques.
- CNIL, Travailler avec un sous-traitant : encadrement contractuel entre responsable de traitement et sous-traitant.
- CNIL, Article 28 du RGPD : obligations du responsable de traitement et du sous-traitant.
- ANSSI, Guide d'hygiène informatique : repères généraux sur les mises à jour, sauvegardes, accès et sécurité numérique.
- Cybermalveillance.gouv.fr : sensibilisation des entreprises, bonnes pratiques et assistance en cas d'incident cyber.