Security Policy - Crossmedia House
Versie: 1.1
Datum: 4-3-2025

---

1. Inleiding

Crossmedia House zet zich in voor de veiligheid van de WordPress-websites die zij ontwikkelt en beheert. Dit document beschrijft de beveiligingsmaatregelen en de verantwoordelijkheden van Crossmedia House en haar klanten, met als doel het minimaliseren van beveiligingsrisico's zoals hacks en datadiefstal.

Hoewel Crossmedia House proactief beveiligingsmaatregelen treft, is absolute veiligheid niet te garanderen. Dit beleid beschrijft hoe we risico's minimaliseren en omgaan met beveiligingsincidenten.

---

2. Hosting en Serverbeheer

- Crossmedia House host geen websites zelf, maar maakt gebruik van een **derde partij** voor hosting – Vimexx b.v. hierna hostingpartner genoemd.
- Met deze hostingpartner is een **managed service contract** afgesloten, waarbij:
    - De server periodiek wordt onderhouden en bijgewerkt.
    - Beveiligingspatches en updates tijdig worden uitgevoerd.
    - Monitoring plaatsvindt om beveiligingslekken te detecteren en te verhelpen.
    - Hostingpartner zal persoonsgegevens bewaren van Crossmedia House zoals volgt uit de fiscale bewaarplicht op de servers van Vimexx b,v, gevestigd in Nederland. Deze wettelijke verplichting houdt in dat bron-, afgeleide- en vaste gegevens minimaal 7 jaar moeten worden bewaard. Persoonsgegevens die niet onder deze kwalificatie vallen zullen na 30 dagen van de servers en systemen van de Verwerker worden verwijderd. Bij het beëindiging van een overeenkomst voor hosting met Crossmedia House, als gevolg van opzegging dan wel ontbinding, is hostingpartner gerechtigd om per direct alle opgeslagen gegevens te wissen of ontoegankelijk te maken en alle accounts op te heffen.

- **Verantwoordelijkheid:**

    - Crossmedia House is **niet verantwoordelijk** voor serverbeveiligingsrisico's die te wijten is aan nalatigheid door de hostingpartner, Wel zal Crossmedia House direct actie ondernemen wanneer bekend is dat er beveiligingsrisico's zijn en dit in samenwerking met de hostingpartner verhelpen door patches en/of updates.
    - De hostingpartner meldt beveiligingsincidenten, DDoS-aanvallen en brute force aanvallen via een **storings-URL**.
    - Indien een storing de klanten van Crossmedia House raakt, worden zij hierover geïnformeerd via een **digitale mailing**. De hostingpartner zal storingen, hacks en/of aanvallen mededelen via een NOC status systeem (https://status.vimexx.nl/) – Crossmedia House is geabonneerd op de NOC status lijn en ontvangt direct een melding per mail bij een storing of ander calamiteit.

---

3. Communicatie bij Storingen en Updates

- **Werkdagen:** Maandag t/m vrijdag van **08:30 - 17:00 uur**.
- **Weekend:** Storingen kunnen gemeld worden via **support@crossmediahouse.nl**.
- Bij updates of migraties die mogelijk **korte downtime** veroorzaken, informeert Crossmedia House klanten tenminste 48 uur van te voren via e-mail.

---

4. Beheer en Onderhoud van WordPress-Websites

Crossmedia House onderhoudt en update WordPress-websites om beveiligingsrisico's te beperken.

Updates en onderhoud:

- Minimaal **één keer per maand** worden WordPress-core, plugins en thema's geüpdatet.
- Kritieke beveiligingspatches worden binnen 5 werkdagen uitgevoerd nadat kennis is genomen van de update.

Back-ups:

- Websites gehost via de hostingpartner krijgen minimaal **één keer per 24 uur een volledige back-up**.
- Backups worden 1x per maand willekeurig getest
- Backups worden maximaal 60 dagen lang bewaard.
- Backups zijn zichtbaar via een Backup file browser zodat Crossmedia House inzage heeft in op welke dag en tijdstip een backup is gemaakt.

Toegangsbeheer:

- Het maken van beheerders tot de backend van websites wordt uitsluitend door Crossmedia House verstrekt en in opdracht van de opdrachtgever. Hierna kunnen deze beheerders, ook andere mensen als beheerder uitnodigen. Het is de verantwoordelijkheid van de opdrachtgever dat deze zorgvuldig omgaat met de inloggegevens en niet zomaar iedereen toegang geeft tot de backend van de website.
- Crossmedia House is **niet verantwoordelijk** voor acties uitgevoerd door gebruikers die toegang hebben gekregen via een beheerdersrol die de opdrachtgever heeft toegekend aan iemand anders .
- Crossmedia House is **niet verantwoordelijk** voor gebruikers die zij niet heeft aangemaakt en die mogelijk bestanden aanpassen of plugins installeren zonder overleg, of tegen het advies van Crossmedia House in.

---

5. FTP- en Bestandsbeheer

- **FTP-toegang** wordt gebruikt om websitebestanden aan te passen, zoals HTML, CSS of plugin-updates.
- Deze FTP-accounts worden **uitsluitend beheerd door Crossmedia House** en kunnen op elk moment **in- en uitgeschakeld** worden.
- Websites gehost door Crossmedia House worden altijd voorzien van een **SSL-certificaat**.
- Voor elke website wordt op de server een **security.txt-record** geplaatst met de contactgegevens van de security officer of de eindklant.

---

6. Beheer van Formulieren en Gegevensopslag

- **IP-adressen worden niet opgeslagen.**
- **Verantwoordelijkheid:**
    - Klanten die andere of externe plugins gebruiken om formulieren te maken en beheren, zijn verantwoordelijk voor de beveiliging en verwerking van ingezonden gegevens.
    - Crossmedia House kan gevraagd worden voor advies of ondersteuning om deze formulieren wel veiliger te maken.
- Formulieren die Crossmedia House gebruikt hebben standaard een bewaartermijn van de inzendingen van 30 dagen en worden voorzien van bijvoorbeeld reCaptcha of andere beveiligingstools.

---

7. Verantwoordelijkheid van de Klant

- Klanten die **zelf plugins installeren of beheren**, dragen zelf verantwoordelijkheid voor mogelijke beveiligingsrisico's.
- Crossmedia House adviseert om uitsluitend **betrouwbare en geüpdatete plugins** te gebruiken.
- Klanten zijn verantwoordelijk voor het beheer van hun eigen wachtwoorden en gebruikersaccounts.
- Indien CMH onveilige plugins ontdekt zal deze worden gedactiveerd in overleg met de klant en hiervoor een alternatief aandragen.
- Indien klant onveilige plugins blijft gebruiken of installeren is CMH gerechtigd om de overeenkomst te ontbinden.

---

8. Aanvullende Beveiligingsmaatregelen

Indien gewenst kan Crossmedia House extra beveiligingsmaatregelen implementeren op aanvraag van de opdrachtgever.

Mogelijke maatregelen:

- **2-factor authenticatie** activeren voor WordPress-gebruikers.
- **Aanpassen van de WordPress inlog-URL** om brute force aanvallen te verminderen.
- **Maximaal drie mislukte inlogpogingen** toestaan om accounts te beschermen.

- **Gebruik van uitsluitend sFTP-verbindingen** waarbij alleen specifieke IP-adressen toegang krijgen.
- **Formulierinzendingen met persoonsgegevens direct verwijderen** in plaats van 30 dagen op te slaan.
- **Het gebruik van privacy veilig analytics tools** zoals Simple Analytics in plaats van bijvoorbeeld Google Analytics.
- **DNSSEC activeren op het domeinnaam**, mits het domein via Crossmedia House is geregistreerd of de huidige domeinnaamhouder DNSSEC ondersteunt.

Indien een klant extra beveiligingsmaatregelen wenst, kan dit in overleg met Crossmedia House worden geïmplementeerd.

---

9. Slotbepalingen

Dit security policy document is bedoeld om transparantie te bieden over de beveiligingsmaatregelen die Crossmedia House neemt. Klanten dienen zich bewust te zijn van hun eigen verantwoordelijkheid bij het beheren van hun website.

Voor vragen of beveiligingsincidenten kan contact worden opgenomen via **support@crossmediahouse.nl**.

Crossmedia House behoudt zich het recht voor om dit document periodiek te actualiseren op basis van nieuwe inzichten en ontwikkelingen. Crossmedia House zal bij een substantiële wijziging van dit document de klanten middels een mailing op de hoogte stellen.

Indien klant aanvullende of aangepaste afspraken wil kan hiervoor een separate overeenkomst worden afgesloten.

Crossmedia House
Crossmediahouse.nl
Lansinkesweg 4
7553AE Hengelo
053-8512665
info@crossmediahouse.n;l