

COTTONCLOUD SECURITY STANDARD

WordPress pod kontrolou. Stav opatrení otvorene.



Interný rámec riadenej WordPress prevádzky. Pri každom opatrení uvádzame jeho reálny stav k 28. 7. 2026.

Ako čítať stavy

POTVRDENÝ ROZSAH

Nasadenie je potvrdené pre uvedený rozsah. Konkrétny web overujeme samostatne; samotná prítomnosť funkcie v kóde nestačí.

V ZAVÁDZANÍ

Zdrojový modul alebo proces existuje, no ešte neprešiel kompletným zákaznickým release, E2E kontrolou a pilotom.

PODĽA PLÁNU

Opatrenie sa realizuje až po technickom a zmluvnom potvrdení konkrétneho rozsahu.

Doložený základ - kód alebo potvrdený rozsah

01 Kontrolovaný základ stacku

Hlavné funkcie stavíme na CottonCloud komponentoch. Potrebné rozšírenia tretích strán vyberáme cielene a závislosti minimalizujeme.

02 Formuláre s kontrolami

Lead formuláre používajú nonce, honeypot, sanitizáciu vstupov a limit pokusov. Opatrenia znižujú riziko, nie sú zárukou nulového spamu.

03 Podpísané licenčné požiadavky

Licenčné API podporuje HTTPS kontrolu, čerstvosť časovej pečiatky, HMAC-SHA256 podpis a rate limit.

04 Prihlásenie a aplikačný hardening

Odkaz + PIN a allowlist používame v potvrdenom rozsahu. Prísny režim blokuje heslový wp-login aj správcovi; klient obnoví prístup záložným kódom + PIN a núdzový break-glass je časovo obmedzený a auditovaný. Site Protection nenahrádza WAF.



Tieto opatrenia nie sú certifikáciou, penetračným testom ani zárukou nulového rizika. Stav nasadenia sa overuje pre každý web osobitne.

TRANSPARENTNÝ STAV

Lokálne moduly pred pilotom

Zálohy a monitoring sú implementované v lokálnom kandidáte a default vypnuté. Na konkrétnom webe ich označíme za aktívne až po konfigurácii, testoch a úspešnom zdokumentovanom behu.

V ZAVÁDZANÍ**Databázová záloha**

Modul vie vytvoriť a overiť gzip zálohu databázy podľa nastaveného rozvrhu. Je default vypnutý a vyžaduje vedomú per-site aktiváciu.

V ZAVÁDZANÍ**Voliteľné šifrovanie a off-site**

Po samostatnej konfigurácii podporuje XChaCha20-Poly1305 alebo AES-256-GCM a kópiu na S3, SFTP či FTPS. Bez kľúča nešifruje; bez cieľa nič mimo server neodosiela.

V ZAVÁDZANÍ**Overenie archívu a off-site kópie**

Zapnutý modul kontroluje čitateľnosť archívu a pri off-site prenose stiahne kópiu späť a porovná SHA-256. Na konkrétnom webe to tvrdíme až po úspešnom zaznamenanom behu.

V ZAVÁDZANÍ**Obnova a skúška obnovy**

Obnova a restore drill sú v lokálnom kandidáte. Plná skúška vyžaduje izolovanú testovaciu databázu; bez nej prebehne len suchá kontrola dumpu. Zatiaľ nejde o overenú službu.

V ZAVÁDZANÍ**Monitoring a HTML prehľad**

Moduly po per-site aktivácii sledujú vybrané verzie a súbory a vedia pripraviť HTML prehľad. Nie sú externým uptime monitoringom, 24/7 alertingom ani všeobecným SLA.

V ZAVÁDZANÍ**Release, aktivácia a dôkaz**

Zálohy ani monitoring neoznačujeme za aktívne plošne. Potrebujú zákaznícky release, end-to-end overenie, per-site konfiguráciu a dôkaz úspešného behu na konkrétnom webe.

Release gate pre všetky rozpracované oblasti

1

Security review

2

Zákaznícky build

3

E2E test

4

Pilot a dôkaz

Zálohy a monitoring neoznačujeme za aktívnu službu, kým neprejdú release gate a pilotom na konkrétnom webe.

MERATEĽNÁ SLUŽBA

Riadená starostlivosť má jasný rozsah

Potvrdíme iba opatrenia, ktoré vieme na konkrétnom projekte reálne zaviesť, overiť a prevádzkovať.

PODĽA PLÁNU

Inventár a baseline

Komponenty, verzie, prístupy, hosting a východiskový stav opatrení.

PODĽA PLÁNU

Aktualizačný postup

Rizikové zmeny testujeme na stagingu, ak je pre projekt dostupný, a dohodneme postup návratu.

PODĽA PLÁNU

Zálohovanie a obnova

Úložisko, retenciu, šifrovanie a skúšku obnovy uvádzame až po reálnom zavedení a overení.

PODĽA PLÁNU

Monitoring

V ponuke sa určia signály, frekvencia kontroly, upozornenie a zodpovedná osoba. Bez všeobecného sľubu 24/7.

PODĽA PLÁNU

Incident a reakčný čas

Cieľové časy platia iba v rozsahu konkrétnej ponuky alebo zmluvy. Bez osobitnej dohody nejde o pohotovosť 24/7.

PODĽA PLÁNU

Bezpečnostný prehľad

Po zavedení dátových zdrojov môže obsahovať kontroly, zistenia, zmeny a otvorené riziká podľa servisného plánu.

Najprv zistíme stav.

Potom potvrdíme, čo vieme prevádzkovať.

Pošlite URL a stručný kontext. Navrhne priority, rozsah správy a merateľný bezpečnostný plán pre váš WordPress.

[COTTONCLOUD.SK/BEZPECNOST](https://cottoncloud.sk/bezpecnost)

ahoj@cottoncloud.sk · 0948 483 969

Dôležité: bezpečnosť nie je absolútny stav. Rozsah monitoringu, zálohovanie, testovanie obnovy a reakčné časy závisia od servisného plánu a technických možností projektu.