Veiligheid & Privacy in 5 muren

Platform — gebouwintelligentie waarvan verzekeraars mogen uitgaan

Muur 1 — Tenant-isolatie

Elke klantorganisatie ziet uitsluitend de eigen gegevens; geen enkel scherm, rapport of export bereikt een andere organisatie.

Muur 2 — Gebouw-compartimentering

Binnen een organisatie gelden per gebouw aparte rechten: wie één complex beheert, ziet nog geen meter van een ander complex.

Muur 3 — Pincode op deellinks

Externe deellinks kunnen op Niveau 3 alleen met pincode worden geopend; een doorgestuurde link is zonder code waardeloos.

Muur 4 — SHA-256-zegel & auditlog

Elk MJOP-rapport en elke export draagt een cryptografisch zegel (SHA-256) met tijdstempel, en elke handeling staat in de auditlog.

Muur 5 — Onderdrempel-bewaking

Sessieduur, tweefactorverplichting en inactiviteitsdrempels worden afgedwongen; elke gebruiker kan zelf strikter, nooit laxer.

Zelf instelbaar: Beveiligingsniveau 1 t/m 4

Niveau 1 — Basis / Toegankelijk
2FA optioneel · sessie tot 168 uur · uitnodiging 30 dagen · inactief na 180 dagen

Niveau 2 — Verhoogd
2FA voor beheerders · sessie tot 24 uur · uitnodiging 14 dagen · inactief na 90 dagen

Niveau 3 — Strikt
2FA voor iedereen · sessie tot 8 uur · pincode op deellinks · uitnodiging 7 dagen, inactief na 60 dagen

Niveau 4 — Enterprise / Op maat
alle beleidsopties zelf instellen naar eigen norm

Wat het zegel betekent
Rapporten en exports zijn cryptografisch verzegeld: de SHA-256-handtekening over de cijfers staat in het document én in de auditlog, met tijdstempel. Eén gewijzigd cijfer maakt het zegel ongeldig — een verzekeraar of accountant kan de integriteit controleerbaar vaststellen.

https://fps-one.nl — © 2026 Platform · Alle rechten voorbehouden.