Beveiliging van uw data in Toxic 2.0

TOXIC 2.0 is een moderne web applicatie waarbij vanaf het begin af aan rekening is gehouden met beveiliging. Beveiliging staat centraal bij de ontwikkeling van de applicatie, het opzetten van de hosting-servers en natuurlijk het doorlopende onderhoud.

Hierbij wordt niet alleen rekening gehouden met het afweren van onbevoegden (hackers), maar ook met de privacy van en wie toegang heeft tot uw gegevens.

Er zijn verschillende lagen van bescherming ingebouwd in TOXIC om de maximale beveiliging te waarborgen. Het betreft hier zowel technische beveiliging als protocollaire afspraken en actieve monitoring van TOXIC.

Daarnaast beschermt TOXIC uw gegevens actief tegen calamiteiten zoals hardware of netwerk-storingen. Dit gebeurt o.a. door 24/7 monitoring en het dagelijks automatisch maken van ge-encrypte back-ups.

SSL

Toegang tot TOXIC verloopt via SSL. Deze beveiligde verbinding zorgt ervoor dat al het verkeer tussen u en Toxic encrypted is. Het is voor onbevoegden niet mogelijk om communicatie tussen uw PC en Toxic te onderscheppen.

GEVALIDEERD INLOGSYSTEEM

TOXIC gebruikt het GA/GAIA authenticatiesysteem. Deze is ontwikkeld op het toon aangevende *Central Authentication Service* (CAS) project van *JASIG* en de *Yale universiteit*. GA/GAIA is een bewezen systeem dat continue onderhouden wordt en garandeert een veilige opslag van uw gebruikersgegevens en authenicatie.

BEVEILIGING CENTRAAL BIJ DE ONTWIKKELING

Tijdens de ontwikkeling van TOXIC staat beveiliging centraal. Het ontwikkelteam achter TOXIC monitort het *Open Web Application Security Project* (OWASP) en voert haar aanbevelingen door op TOXIC. TOXIC is ontwikkeld met het voorkomen van risico's zoals SQL Injections, Cross-site scripting, et cetera.

SOLIDE HOSTINGSPARTNER

TOXIC is ondergebracht bij een hostingpartner met een uitstekende track-record omtrent beveiliging. De servers zijn geplaatst binnen *Europa.* Er zijn strikte afspraken omtrent de toegang en beveiliging van de data. De servers worden 24/7 gemonitord door de hostingpartner. De servers worden up-to-date gehouden met security-patches.

BEVEILIGINGSPROTOCOL

Er is een beveiligingsprotocol aanwezig omtrent de accountability en toegang tot de binnen TOXIC aanwezige data. Hierin is opgenomen o.a. wie toegang tot de data heeft, hoe om te gaan met vertrouwelijke data, maar ook de veiligheid van backups en het voorkomen van data-verlies bij calamiteiten.