

Programma van Eisen Non Functionals

Informatiebeveiliging en Privacy - Toegang	Accounts dienen persoonlijk te zijn, derhalve is het gebruik van generieke accounts niet toegestaan. Persoonlijke accounts mogen niet overgedragen worden. Deze eis is relevant indien (management)informatie wordt aangeboden via een portaal
Informatiebeveiliging en Privacy - Toegang	Inschrijver heeft maatregelen getroffen ten behoeve van het voorkomen van misbruik van informatie door personeel en (onder)aannemers en het ten onrechte verstrekken van informatie aan onbevoegden. Deze maatregelen kunnen zowel technisch, op personele vlak, maar ook procesmatig zijn.
Informatiebeveiliging en Privacy - Toegang	De aangeboden oplossing dient ondergebracht te zijn binnen de EER (Europese Economische Ruimte).
Informatiebeveiliging en Privacy - Toegang	De aangeboden oplossing dient logisch gescheiden te zijn van andere partijen.
Informatiebeveiliging en Privacy - Algemeen	Er zijn maatregelen getroffen om de dreiging van een hack/inbreuk en van kwaadaardige software te mitigeren. •AntiVirus software •Firewall met IDS/IPS •DLP •SIEM SOC – actieve monitoring & opvolging
Informatiebeveiliging en Privacy - Algemeen	Hardening van systeem en proces is ingericht en toegepast. Aantoonbaar door: * Inrichten volgens hardenings baselines (CIS) * Uitschakelen van services die niet nodig zijn * Uitschakelen van poorten die niet nodig zijn * Uitschakelen van datanetwerk services die niet nodig zijn * Uitschakelen van default access points die niet nodig zijn * Uitschakelen van default accounts die niet nodig zijn
Informatiebeveiliging en Privacy - Algemeen	Inschrijver draagt zorg dat gedurende de looptijd van de overeenkomst de dienst en/of product gedurende de gehele levenscyclus adquaat wordt onderhouden en beheerd. Verdere specificatie vindt plaats in SLA.
Informatiebeveiliging en Privacy - Algemeen	Inschrijver is verplicht om 'hoog risico beveiligingsincidenten' (hoge kans en hoge impact, zoals ransomware aanvallen) binnen een dag te melden aan de gemeente Tilburg en maximaal binnen 1 kalenderweek op te lossen. Dit geldt ook voor afwijkend systeemgedrag met hoog risico's.
Informatiebeveiliging en Privacy - Algemeen	Uitzonderingen op de eisen van informatiebeveiliging dienen door Inschrijver vooraf besproken en goedgekeurd te worden door Opdrachtgever. Deze uitzonderingen worden vastgelegd, voorzien van motivatie en risicoanalyse. Opdrachtgever stemt dit af met onder andere aanvrager, leverancier, iso/ciso en de business proceseigenaar.

Archief en Informatiebeheer	Opdrachtgever blijft eigenaar van de gegevens die verwerkt worden in het kader van de uitvoering van de gemeentelijke ta(a)k(en) in de oplossing. Dat betekent dat deze gegevens te allen tijde uit het systeem geëxporteerd moeten kunnen worden en daarna uit het systeem verwijderd.
Archief en Informatiebeheer	De aangeboden oplossing beschikt over de mogelijkheid om informatieobjecten (dossiers) van andere opdrachtgevers/zorgdragers onderscheidend van de informatieobjecten van de gemeente Tilburg vast te leggen.