Bijlage Technische en organisatorische beveiligingsmaatregelen DUO

De Opdrachtnemer is verplicht passende technische en organisatorische maatregelen te nemen ter beveiliging en om de maatregelen aan te tonen. Deze bijlage geeft een beknopte beschrijving en opsomming van die maatregelen. Onderstaande zes onderdelen bieden een richtlijn. Indien er niet wordt voldaan aan onderstaande richtlijnen dient uitgelegd te worden op welke wijze er wordt gewerkt, comply or explain.

Algemeen:

- Aantoonbaar voldoen aan BIO/ ISO27001
- Indien n.v.t TTP verklaring of right to audit
- Systemen zijn voorzien van een BIV (Beschikbaarheid, Integriteit en Vertrouwelijkheid) classificatie

Toegang:

- Logische toegang tot systemen met informatie van DUO alleen op basis van need-to-know.
- De leverancier stelt een autorisatiematrix op. Hierop wordt gemonitord en gerapporteerd.
- Er is een scheiding tussen Ontwikkeling, Test, Acceptatie en Productie.
- Beheerders hebben geen toegang tot de (persoons) gegevens in het systeem
- Er wordt uitsluitend gebruik gemaakt van tot een persoon herleidbare inloggegevens
- Fysieke toegang tot systemen alleen door middel van een toegangscontrole systeem

Continuïteit planning:

- Systemen worden voorzien van een back-up die op een fysiek andere locatie wordt bewaard.
- De back-up dient versleuteld te zijn en op een gecontroleerde wijze vervoerd te worden.
- Er is een goedgekeurd DRP (Disaster Recovery Plan) opgesteld

Beheersmaatregelen:

- Er is patchmanagement ingericht, kritieke patches worden z.s.m. geïnstalleerd. Afwijkingen hierin worden gerapporteerd richting DUO
- Wijzigingen volgen het wijziging proces en vinden plaats in het vooraf afgesproken onderhoud window
- Systemen worden gecontroleerd op kwetsbaarheden, hierop wordt gerapporteerd en worden in overleg verholpen
- Beveiliging incidenten worden gerapporteerd richting DUO en volgen het incident proces

Programmatuur:

- Programmeren met inachtneming OWASP
- Door DUO uitgevoerde pentest wordt toegestaan
- De broncode wordt bescherm tegen onbevoegde toegang en blijft eigendom van DUO

Beveiliging:

- Communicatie vindt uitsluitend plaats over een versleuteld kanaal
- Indien de systemen (bijzondere) persoonsgegevens bevatten wordt gebruik gemaakt van versleutelde opslag