

## Artikel XX: Cybersecurity

1. Opdrachtnemer is bekend met het beleid van het Waterschapshuis met betrekking tot wachtwoordgebruik, versleutelingsmethoden en classificatie van gegevens en past deze waar nodig toe.
2. Opdrachtnemer dient, daar waar Opdrachtgever niet verwijst naar specifieke beveiligingsrichtlijnen bij de te treffen maatregelen, de richtlijnen uit de meest recente versie van de NEN-ISO/IEC 27002 norm aan te houden.
3. Opdrachtnemer dient voor ten minste alle cybersecurityprocessen genoemd in dit artikel aantoonbaar de verantwoordelijkheden, taken en bevoegdheden op de daartoe geëigende plaatsen binnen de (project)organisatie te beleggen.
4. Opdrachtnemer dient van het Personeel te eisen dat het zich houdt aan het beleid voor wachtwoordgebruik van Opdrachtgever bij het gebruiken van authenticatiegegevens gerelateerd aan de te leveren Diensten.
5. Opdrachtnemer dient een aantoonbaar operationeel geborgd proces te hebben voor versleutelen van gegevens op mobiele apparatuur betrokken bij de te leveren Diensten waarbij rekening wordt gehouden met de classificatie van deze gegevens en actualiteit van de veiligheid van de gebruikte versleutelingsmethoden.
6. Opdrachtnemer dient over operationeel geborgde processen te beschikken voor het veilig verwijderen van media, transport van media en het beheer van verwijderbare media, betrokken bij de te leveren Diensten, in overeenstemming met het classificatieschema van Opdrachtgever.
7. Opdrachtnemer dient aantoonbaar te beschikken over een operationeel geborgd proces voor het vernietigen van data op media bij afvoeren of vervangen van (delen van) informatiesystemen die deze media bevatten en betrokken zijn bij de te leveren Diensten.
8. Opdrachtnemer dient aantoonbaar operationeel geborgde beleidsregels, procedures en beheersmaatregelen te hebben ter bescherming van het informatietransport betrokken bij de te leveren Diensten, dat via alle soorten communicatiefaciliteiten verloopt.
9. Gegevens of programmatuur van Opdrachtgever, of door deze gegenereerde metadata, welke zich bevinden op informatiesystemen van Opdrachtnemer, is en blijft ten alle tijden eigendom van Opdrachtgever. Indien gegevens door Opdrachtgever aan Opdrachtnemer zijn verstrekt, mag Personeel dit alleen gebruiken voor het doel waarvoor dit is gebeurd.
10. Opdrachtnemer dient aantoonbaar operationeel geborgde processen te hebben voor het vernietigen van gegevens of programmatuur van Opdrachtgever op apparatuur en alle back-up media van Opdrachtnemer, na contractbeëindiging tussen beide partijen.
11. Wanneer gegevens of programmatuur van Opdrachtgever zich bevinden op informatiesystemen van Opdrachtnemer, dient Opdrachtnemer aan te geven waar deze informatiesystemen zich bevinden. Indien deze zich buiten de EU bevinden, mag dit uitsluitend in landen waar een passend niveau van gegevensbescherming wordt geboden; welke landen dit zijn, is bepaald door de Europese Commissie
12. Indien Opdrachtgever of derde partij verantwoordelijk is voor het verschaffen van de fysieke of logische toegang tot informatie verwerkende faciliteiten, dan dient Opdrachtnemer zich te houden aan de door Opdrachtgever of derde partij gehanteerde toegangsprocedure.
13. Wanneer gegevens van Opdrachtgever zich bevinden op informatiesystemen van Opdrachtnemer, dient bij contractbeëindiging tussen deze beide partijen, de Opdrachtnemer assistentie te leveren bij de overdracht van deze informatie naar de nieuwe leverancier of terug naar Opdrachtgever.
14. Opdrachtnemer dient aantoonbaar operationeel geborgd te hebben dat Personeel een opleiding en -training op het gebied van cybersecurity beveiligingsbewustzijn heeft ontvangen passend bij de aard van de uit te voeren werkzaamheden, alsmede jaarlijkse bijscholing krijgt, waarin ten minste ook persoonlijke verantwoordelijkheid en specifieke beveiligingskaders van Opdrachtgever ter sprake komen.

15. Opdrachtnemer dient een aantoonbaar operationeel geborgd proces te hebben voor het definiëren van verantwoordelijkheden en taken met betrekking tot informatiebeveiliging voor de te leveren Diensten en dient naar het Personeel te communiceren dat:

1. deze van kracht blijven na beëindiging of wijziging van het dienstverband;
2. deze ten uitvoer moeten worden gebracht.