



## Bijlage 8

# notitie

Informatiebeveiliging, toegang en gedrag  
PR 18017 - renovatie PI Lelystad

**Rijksvastgoedbedrijf**  
Directie Transacties & Projecten  
Afdeling Projecten 2

Stationsplein-west 30  
6811 KM Arnhem  
Postbus 16169  
2500 BD Den Haag  
[www.rijksvastgoedbedrijf.nl](http://www.rijksvastgoedbedrijf.nl)

**Datum**  
1 maart 2024

Deze notitie is, in overleg met DJI – FHI en Locatie opgesteld, met betrekking tot het inzetten van externe adviseurs en de kaders die van toepassing zijn ten behoeve van informatiebeveiliging, toegang en gedrag. In deze notitie staan de kaders waarbinnen de werkzaamheden door de externe adviseurs uitgevoerd moet worden.

Voor dit project is op een deel de rubricering “Departementaal Vertrouwelijk” (DEP-V) vastgesteld. Voor dit projectdeel zijn nadere specifieke eisen vastgelegd in de overeenkomst.

### Voorwaardelijke maatregelen:

#### Organisatie:

- ☒ Medewerkers dienen vooraf gescreend te zijn middels een antecedentenonderzoek (VOG) voor toegang tot de PI Lelystad;
- ☒ De geheimhoudingsverklaring is ondertekend door een organisatie bestuurder (kvk). De geheimhoudingsverklaring is ook van toepassing voor de onderaannemers e.d;
- ☒ Er is een Informatiebeveiligingsplan opgesteld.

#### Personeel:

- ☒ Iedereen die in aanraking komt met projectinformatie beschikt over een VOG die niet ouder is dan 5 jaar;
- ☒ Iedereen moet zich kunnen legitimeren door middel van een geldig legitimatiebewijs voordat zij in aanraking komen met projectinformatie of toegang krijgen tot de inrichting.
- ☒ Organiseren van bewustwordingssessie voor personeel

#### Fysiek:

- ☒ Informatie wordt opgeslagen in een kast met slot;
- ☒ De ruimte waarin gewerkt wordt met DEP-V. informatie is een afgesloten ruimte en alleen toegankelijk voor direct betrokkenen;
- ☒ Het in het bezit hebben van een mobiele telefoon, fototoestel, audioapparatuur, opname apparatuur of andere elektronische apparatuur binnen of op terrein van de inrichting is verboden. Voor specifiek gebruik kan bij gebruiker dispensatie worden aangevraagd.

Cyber:

- ☒ Voor informatie welke opgeslagen is in de Cloud, maar ook lokaal, geldt dat de informatie. "in rust" goed encrypted moet zijn;  
(betekenis encrypted: informatie is versleuteld op basis van een willekeurig algoritme)
- ☐ Alle communicatie dient encrypted te zijn;
- ☒ Online communicatie vindt uitsluitend plaats via Webex of microsoft teams.
- ☒ (digitale) Informatie wordt enkel gedeeld middels door het Rijk beschikbaar gestelde platforms (SWR, secure transfer ed.).

Aandachtspunten zijn:

- ☒ Werken met bedrijven die informatiebeveiliging onderdeel maken van het proces/project;  
Bijvoorbeeld door te werken met organisaties die: Werken met beveiligde bedrijfsdocumenten en/of werken aan bewustwording en veiligheidsrisico's
- ☒ Functie en verantwoordelijkheid zijn bepalend voor toegankelijkheid tot informatie;
- ☒ Uitsluitend werken met vertrouwelijke applicaties en uitsluitend informatie delen in vooraf gecommuniceerde werkomgevingen.

Gedrag:

- ☒ Gebruik je gezond verstand.
- ☒ Houd voor jezelf dat je aan dit project werkt.
- ☒ Voer geen gesprekken in het openbaar.
- ☒ Met het project wordt niet geadverteerd en wordt geen publiciteit gezocht.
- ☒ Geen namen op documenten.
- ☒ Geef geen namen door.
- ☒ Geen sociale media en openbare bronnen.