Programma van Eisen

Informatieveiligheid verbindingsmiddelen VRU

Kenmerk: 000009232
Datum: 17-11-2026
Versie: Definitief

Veiligheidsregio Utrecht

vru.nl

1 Eisen informatieveiligheid

Alle onderstaande eisen gelden voor zowel perceel 1 als voor perceel 2.

Nr	Omschrijving
1.1-1	De opdrachtnemer beschikt over een incidentprocedure voor informatiebeveiligingsincidenten en informeert de VRU zo spoedig mogelijk indien zich een incident voordoet dat betrekking heeft op de dienstverlening.
1.1-2	De opdrachtnemer informeert de VRU tijdig over wijzigingen in de dienstverlening die impact kunnen hebben op het gebruik of de beveiliging van de oplossing of dienst.
1.1-3	Opdrachtnemer gaat vertrouwelijk om met alle door de VRU verstrekte informatie, gebruikt deze uitsluitend voor het uitvoeren van de dienstverlening en waarborgt dat onderaannemers contractueel zijn gebonden aan passende geheimhoudings- en informatiebeveiligingsverplichtingen.
1.1-4	Opdrachtnemer beoordeelt kwetsbaarheden en beveiligingsupdates tijdig op relevantie voor de dienstverlening en voert, afhankelijk van de aard en het risico, passende herstel-, patch- of mitigerende maatregelen binnen een passende termijn door.
1.1-5	Opdrachtnemer beschermt vertrouwelijke en gevoelige gegevens tijdens opslag (data at rest) en overdracht (data in transit) met passende cryptografische maatregelen, waaronder versleuteling van gegevensopslag en beveiligde verbindingen voor gegevensoverdracht.
1.1-6	Opdrachtnemer beschikt over passende continuïteits-, back-up- en herstelvoorzieningen voor de dienstverlening en kan op verzoek aantonen hoe verstoringen worden beheerst en hoe de herstelbaarheid van gegevens en systemen die betrekking hebben op de dienstverlening periodiek wordt getoetst.
1.1-7	Indien ten behoeve van de dienstverlening API-koppelingen worden toegepast, is de API-documentatie actueel en correct, wordt deze op verzoek beschikbaar gesteld aan de VRU en zijn de API-koppelingen, inclusief de bijbehorende authenticatiegegevens, adequaat beveiligd.
1.1-8	De oplossing genereert logbestanden waarin, voor zover relevant, minimaal gebruikersidentiteit, datum en tijd van geslaagde en mislukte inlogpogingen, herkomst van de toegangspoging en relevante toegangs- en systeemactiviteiten worden vastgelegd.
1.1-9	Opdrachtnemer maakt inzichtelijk wat de ondersteuningsperiode en end-of-life datum zijn van de oplossing, voor zover relevant voor de dienstverlening, en informeert de VRU tijdig over wijzigingen daarin.
1.1-10	Gegevens die door of namens de VRU binnen de dienstverlening worden verwerkt, blijven onder zeggenschap van de VRU. Opdrachtnemer stelt deze gegevens bij beëindiging van de dienstverlening binnen een overeengekomen termijn beschikbaar in een gangbaar en bruikbaar formaat en verwijdert resterende gegevens aantoonbaar en veilig, tenzij wettelijke bewaarplichten anders vereisen.
1.1-11	Opdrachtnemer beschikt over een geldig ISO 27001 certificaat of aantoonbaar gelijkwaardige certificering. Op verzoek toont opdrachtnemer de Verklaring van Toepasselijkheid (SoA) of een vergelijkbaar document. Indien geen certificering aanwezig is, toont opdrachtnemer aan dat aantoonbaar passende informatiebeveiligingsmaatregelen voor de dienstverlening zijn ingericht, afgestemd op de aard en het risiconiveau van de dienstverlening. Dit blijkt minimaal uit: - een beschrijving van organisatorische, menselijke, fysieke en technologische getroffen maatregelen; - ingerichte doelstellingen, monitoring en evaluatie van informatiebeveiliging;

Nr	Omschrijving
	- aantoonbare borging en beheersing van informatiebeveiliging. De toelichting moet naar het oordeel van VRU voldoende aantonen dat passende maatregelen zijn getroffen ter bescherming van informatie.

Colofon

Dit is een uitgave van
Veiligheidsregio Utrecht

Tekst: K. Groenewegen
Ontwerp: Afdeling Communicatie VRU

17 november 2026



Veiligheidsregio Utrecht

vru.nl