EG041 Base-units

Base-units inclusief Verplaatsingsdienst ten behoeve van Verkeershandhaving met Flexflitsers

ROK Bijlage 12

Informatiebeveiligingseisen Base-unit

Versie 1.0, 3 maart 2026

OPENBAAR MINISTERIE

Revisiehistorie

Dit document is een bijlage van Raamovereenkomst EG041.

Versie	OMSCHRIJVING	DATUM	Type*
1.0	Definitieve versie voor publicatie	03-03-2026	

* *Wijziging*: Aanpassing heeft geleid tot een wijziging van de afspraken.
Tekstueel: Aanpassing heeft geleid tot een tekstuele verduidelijking van de afspraken.

Inhoudsopgave

1 Inleiding

1.1 Identificatie

Dit document is Bijlage 12 van Raamovereenkomst EG041 en betreft de Informatiebeveiligingseisen die worden gesteld aan de Base-units, alle onderdelen en componenten daarvan en het eventueel daaraan verbonden computernetwerk.

1.2 Document overzicht

In dit document worden de algemene informatiebeveiligingseisen van EG041 gespecificeerd.

Iedere Eis is weergegeven in een aparte regel die uit twee kolommen bestaat. De eerste kolom bevat een unieke identificatie. Een identificatie bestaat uit de letters ‘Eis’ gevolgd door een uniek volgnummer. In de tweede kolom is de Eis geformuleerd. Daar waar nuttig en/of noodzakelijk is een toelichting opgenomen ter verheldering. Een eventuele toelichting bij een Eis wordt voorafgegaan door het woord 'Toelichting'.

Hieronder is de lay-out van een eis bij wijze van voorbeeld opgenomen:

EIS N	Hier is een eis geformuleerd. *<u>Toelichting:</u>* *Hier staat een toelichting beschreven*

2 Informatiebeveiligingseisen

Inleiding
Om de risico's van datalekken en integriteitschendingen te minimaliseren dient Opdrachtnemer aan tenminste dezelfde normen voor informatiebeveiliging te voldoen als de overheid. Deze normen zijn vastgelegd in de Baseline Informatiebeveiliging Overheid (BIO). Op het moment van schrijven is dit BIO2 (zie bijlage 1). Aanvullend hierop is de ondergrens voor een aantal te nemen maatregelen vastgesteld in dit document.

Audits
Zoals in de ROK is bepaald, is Opdrachtgever gerechtigd tot audits, onder andere om toe te zien op de wijze waarop informatiebeveiligingsmaatregelen worden toegepast en op de rechtmatigheid van de verwerking van Persoonsgegevens.

Onderaannemer
Alle eisen uit dit document zijn ook van toepassing op Onderaannemers van Opdrachtnemer.

Verificatie en validatie
Dit document met Eisen aan de informatiebeveiliging biedt Opdrachtnemer een raamwerk, normen, kaders en maatregelen waaraan Opdrachtnemer zal moeten blijven voldoen, zodat aantoonbaar wordt gemaakt dat de informatiebeveiliging voldoet aan het vereiste beveiligingsniveau op elk moment in de levenscyclus van de EG041 ROK en NOK. Deze verificatie kan gedaan worden door het overleggen van bewijsstukken en/of een verklaring (*comply or explain*).

2.1 Baseline Informatiebeveiliging Overheid

EIS IB-1	De organisatie van de Opdrachtnemer en zijn dienstverlening dienen in opzet, bestaan en werking te voldoen aan de Baseline Informatiebeveiliging Overheid (BIO2, te downloaden op www.bio-overheid.nl). Opdrachtnemer toont dat jaarlijks aan middels een onafhankelijke onderzoek.
EIS IB-2	Informatiebeveiliging en privacy zijn dynamische onderwerpen en de maatregelen dienen vanwege toenemende risico's en bedreigingen via een PDCA-cyclus actueel te worden gehouden.
EIS IB-3	Op de inrichting van het beheer van Informatiebeveiligingsincidenten zijn beheersmaatregelen 5.24 t/m 5.28 van de BIO2 van toepassing.
EIS IB-4	Op het bedrijfscontinuïteitsbeheer zijn de beheersmaatregelen 5.29, 5.30 en 8.14 van de BIO2 van toepassing.
EIS IB-5	Op de inrichting van verantwoordelijkheden bij informatiebeveiliging zijn beheermaatregelen 5.02, 5.03, 5.05, 5.06 en 5.08 van de BIO2 van toepassing.

2.2 Aanvullende eisen

In aanvulling op of invulling van de kaders en maatregelen die in de BIO zijn beschreven, worden hieronder een aantal specifieke en/of aanvullende eisen beschreven.

2.2.1 Algemeen

EIS IB-6	Alle netwerkomgevingen buiten het netwerk van de Base-unit worden beschouwd als 'onvertrouwde zone'. *<u>Toelichting:</u>* *De 'onvertrouwde zone', ook bekend als de externe zone, bevat systemen, die niet onder het beveiligingsregime en de (beheer) verantwoordelijkheid vallen van Opdrachtnemer. Dit impliceert onder andere dat toegang tot het netwerk van de Base-unit altijd met (minimaal) twee-factor authenticatie (2FA) tot stand komt.*
EIS IB-7	Vertrouwelijke gegevens worden altijd versleuteld opgeslagen, ongeacht of deze zich binnen of buiten het netwerk van de Base-unit bevinden.

2.2.2 Cryptografie

EIS IB-8	Indien certificaten worden gebruikt voor informatie-uitwisseling zijn dat certificaten die worden uitgegeven door een door het NCSC of Opdrachtgever geadviseerde partij.
EIS IB-9	Alle gebruikte sleutels en beveiligingsalgoritmen in de Base-unit moeten zo zijn gekozen dat ze tenminste de looptijd van de ROK en NOK voldoende veilig zijn. *<u>Toelichting:</u>* *Zie https://www.keylength.com/en/compare/.*

2.2.3 Communicatie

EIS IB-10	Voor beveiliging worden alleen componenten gebruikt die aantoonbaar voldoen aan geaccepteerde beveiligingscriteria zoals beschreven onder de Open standaarden voor de Nederlandse Overheid of Certificering volgens ISO/IEC 15408 (common criteria).

2.2.4 Intervallen, afstanden, termijnen en versies

EIS IB-11	Maximale periode waarbinnen op de systemen van Opdrachtnemer bijgewerkt wordt: IDS en IPS signatures: 1 dag

Virusdefinities voor systemen en componenten die met het internet verbonden zijn of kunnen zijn.*	1 dag
Virusdefinities voor overige systemen en componenten	2 weken
Securitypatches en –updates voor netwerksystemen en netwerkcomponenten	1 dag
Securitypatches en updates voor overige systemen en componenten	2 weken
Overige Patches en Software updates	In overleg met Opdrachtgever

Maximale intervallen:

Virusscan van opgeslagen data op server	7 dagen
Virusscan van opgeslagen data op mobiele werkplek	7 dagen
Controleren consistentie gerepliceerde informatie	90 dagen
Controle of inactief account verwijderd kan worden	60 dagen
Wijzigen van het wachtwoord	3 maanden
Toegestane periode voor wijzigen van het wachtwoord	14 dagen, of bij eerste login na 14 dagen
Ongeldig maken van het initiële wachtwoord	1 dag
Inschakelen screensaver na inactiviteit	15 minuten

Minimale en maximale waarden:

Minimale afstand tussen redundante systemen	500 meter
Minimale afstand tussen off-line backupmedia	501 meter
Maximale afwijking van UTC van systeemklok	200ms
Maximale afwijking van datum en tijd in logregel	500ms
Minimale versie SNMP	Versie 3
Minimale versie TLS	1.3
Maximaal aantal inlogpogingen	5
Minimale blokkade na maximaal aantal inlogpogingen	10 minuten
Minimale periode rapportage over logging informatie	Maandelijks

Bewaartermijnen logbestanden:

Minimale bewaartermijn voor logbestanden	3 maanden

	Minimale bewaartermijn voor logbestanden bij een (vermoed) beveiligingsincident	3 jaar

3 Bijlagenoverzicht

Dit hoofdstuk bevat een overzicht van de bijlagen.

Bijlage	Toelichting
ROK EG041 B12.1 Baseline Informatiebeveiliging Overheid 2 (PDF-bestand)	De vigerende BIO versie.
ROK EG041 B12.2 Was-wordt lijst BIO-BIO2 (Excel-sheet)	Deel 2 BIO2 in Excel, inclusief een Was-wordt-lijst BIO