Bijlage 22b IB-eisen

Digitale werkplek (DWP) perceel 2
AV-middelen
Kadaster

Directie Governance, Data en Vernieuwing

Kenmerk	
Opdrachtgever	Directie DGV
Auteur	Eelco Schatborn
Versie	1.0
Versiedatum	05-05-2026

IB-eisen AV-middelen

1. Automation & Orchestration

1.1 Connectivity

Network Access Control

Eis 1. Opdrachtnemer dient ervoor te zorgen dat de configuratiebestanden van de door Opdrachtgever aangewezen Connectivityleverancier, inclusief instellingen voor Network Access Control (NAC) authenticatie, op alle door hem beheerde werkplekken, servers, printers/scanners en mobiele apparaten correct worden toegepast, geconfigureerd en up-to-date gehouden. Hierdoor wordt gegarandeerd dat alleen compliant apparaten toegang krijgen tot het Opdrachtgever-netwerk en de bedrijfsservices.

Eis 2. Opdrachtnemer dient ervoor te zorgen dat de benodigde agent en configuratiebestanden van de door het Opdrachtgever aangewezen Connectivity leverancier, inclusief instellingen voor Secure Access Service Edge (SASE), op alle door hem beheerde werkplekken, servers, printers/scanners en mobiele apparaten correct worden toegepast, geconfigureerd en up-to-date gehouden.

1.2 Patch- & Lifecyclemanagement

Opdrachtnemersketen

Eis 3. Indien Opdrachtnemer gebruik maakt van onderaannemers of derde partijen, moet hij aantoonbaar borgen dat deze partijen hetzelfde patchbeleid naleven (door contractuele verplichting of auditverklaring)

Automatisering

Eis 4. Opdrachtnemer moet een geautomatiseerd patchmanagementproces toepassen waarmee updates kunnen worden uitgerold, getest en gemonitord, inclusief logging van installatiestatus.

Afwijkingsprocedure bij incompatibiliteit

Eis 5. Indien een patch niet geïnstalleerd kan worden, moet Opdrachtnemer dit binnen 24 uur melden aan het Opdrachtgever, met een onderbouwde risicoanalyse en herstelplan.

Herijking hardware levensduur

Eis 6. *Uitvoeringseis* - Opdrachtnemer moet waarborgen dat de door hem beheerde systemen voldoende resources beschikbaar hebben om moderne security-technieken effectief te implementeren, beheren en onderhouden.

Mitigerende maatregelen bij vertraging

Eis 7. Indien voor een vastgesteld beveiligingsrisico nog geen patch beschikbaar is, moet de leverancier passende mitigerende maatregelen implementeren binnen de normtijden zoals beschreven in het beleid "License to Operate" van Opdrachtgever.

Eis 8. Indien een patch niet binnen de afgesproken termijn kan worden geïmplementeerd, moet Opdrachtnemer binnen de afgesproken tijden na constatering een mitigerend plan van aanpak opstellen, inclusief

a. Oorzaak van de vertraging
b. Beschrijving van tijdelijke beveiligingsmaatregelen
c. Verwachtte implementatiedatum

Securitypatches

Eis 9. Nieuwe software- en beveiligingsupdates moeten conform het beleid "License to Operate" van Opdrachtgever zijn geïnstalleerd worden op alle relevante systemen. Op moment van schrijven betekent dit dat de laatste versies van systeemsoftware wordt gebruikt. Dus deze is up-to-date: dat wil zeggen de laatste versie is geïnstalleerd en (security) updates conform de SLA geïnstalleerd worden.

Update- en patchbeheer

Eis 10. Opdrachtnemer heeft aantoonbaar effectieve patch- & lifecycle- managementprocessen t.a.v. alle fysieke & virtuele apparaten, systemen, softwareplatformen en alle geïnstalleerde applicaties, waarbij alle onderdelen onder actieve contractuele (security) support vallen van de leveranciers van Opdrachtgever met betrekking tot de producten die vallen onder deze aanbesteding en zo binnen gestelde SLA-tijden van de security patches worden voorzien.

Eis 11. Opdrachtnemer voert volgende type updates uit die buiten het beleid "License to Operate" van Opdrachtgever vallen. Hierbij zijn ook de SLA-tijden benoemd. Dit betreft:

Niveau	Alternatieve termen	Beschrijving	SLA
Medium	Moderate	CVSS-score 4-6,9	< 10 werkdagen
Low	Minor	CVSS-score 0,1-3,9	< 1 maand
Informatief	Notice	Geen direct kwetsbaarheid	1 jaar

Eis 12. Opdrachtnemer moet ervoor zorgen dat op alle door hem geleverde en beheerde ICT-middelen de laatst beschikbare versies van systeemsoftware en applicaties zijn geïnstalleerd, conform het beleid "Bijlage 24 License to Operate 1.0" van Opdrachtgever.

Virusdefinities

Eis 13. Opdrachtnemer moet alle anti-malwareoplossingen minimaal dagelijks moeten monitoren en indien nodig bijwerken met de nieuwste malwaredefinities.

1.3 Vulnerability Management

Vulnerabilityscanning

Eis 14. Opdrachtnemer moet op alle door hem beheerde werkplekken en mobiele apparaten de kwetsbaarheden scanner van Opdrachtgever installeren en correct configureren.

Eis 15. Opdrachtnemer moet de tooling volgens de minimale beveiligingsinstellingen die door Opdrachtgever zijn vastgesteld configureren.

Verwerking bevindingen

Eis 16. Opdrachtnemer dient kwetsbaarheidsbevindingen centraal aanleveren en verwerken binnen het Security Operations platform van Opdrachtgever.

2. Information Security

2.1 Wet & Regelgeving

Naleving Baseline Informatiebeveiliging Overheid (BIO versie 2)

Eis 17. *Uitvoeringseis* - Opdrachtnemer dient te waarborgen dat alle door hem geleverde diensten, systemen, producten en processen die worden ingezet voor of bijdragen aan de uitvoering van deze opdracht, voldoen aan de eisen en beheersmaatregelen zoals vastgelegd in de Baseline Informatiebeveiliging Overheid (BIO versie 2).

Naleving Cyberbeveiligingswet (Cbw / NIS2)

Eis 18. *Uitvoeringseis* - Opdrachtnemer moet garanderen dat alle door hem geleverde diensten, producten, systemen en devices voldoen aan de vereisten van de Cyberbeveiligingswet (Cbw), inclusief de verplichtingen voortvloeiend uit de NIS2-richtlijn, voor wat betreft beveiliging, meldplicht, zorgplicht, en toeleveringsketen en levert een rapportage op waaruit dit blijkt of afwijkt.

Naleving Wet beveiliging netwerk- en informatiesystemen (Wbni)

Eis 19. *Uitvoeringseis* - Opdrachtnemer dient te waarborgen dat alle door hem geleverde diensten, systemen en ondersteunende
infrastructuren die onderdeel uitmaken van de opdracht, voldoen aan de vereisten uit de Wet beveiliging netwerk- en informatiesystemen (Wbni) en de daarop gebaseerde Europese richtlijn NIS2 en levert een rapportage op waaruit dit blijkt of afwijkt.

Aantoonbare naleving

Eis 20. Opdrachtnemer dient naleving van BIO, NIS2 en aanverwante wet- en regelgeving aantoonbaar te maken via geautomatiseerde technische controles.

2.2 Asset Management

Centrale registratie in CMDB

Eis 21. Alle fysieke & virtuele apparaten, systemen, softwareplatformen en applicaties die onderdeel zijn van de dienstverlening aan Opdrachtgever zijn uiterlijk vanaf ingebruikname geïdentificeerd en geregistreerd met vereiste (meta)gegevens in de CMDB van Opdrachtgever conform het CSDM 4.0-data-model.

Dataconsistentie

Eis 22. Opdrachtnemer moet ervoor zorgen dat de data in de CMDB consistent is met andere relevante bronnen (zoals bijvoorbeeld Microsoft Intune)

Datakwaliteit & actualiteit

Eis 23. Opdrachtnemer moet wijzigingen in assetgegevens (zoals status, locatie, eigenaar, of configuratie) binnen 24 uur na wijziging actualiseren in de CMDB.

Integratie & samenwerking

Eis 24. Opdrachtnemer moet de CMDB van Opdrachtgever gebruiken als bron voor Incident Management, Change Management en Problem Management, zodat relaties tussen assets en bedrijfsdiensten inzichtelijk blijven.

Unieke identificatie van assets

Eis 25. Iedere geregistreerde asset moet voorzien zijn van een uniek identificatienummer (bijv. Asset-ID of Configuration Item-ID) dat correspondeert met Opdrachtgever-standaard voor assetnaming.

2.3 Encryptie

Implementatie en Beheer

Eis 26. Opdrachtnemer is verantwoordelijk voor het correct implementeren, beheren en monitoren van alle cryptografische maatregelen op alle relevante systemen en diensten.

Quantum-resistente encryptie

Eis 27. Zodra algemeen aanvaarde en gestandaardiseerde quantum-resistente cryptografische algoritmen (zoals vastgesteld door NIST of vergelijkbare internationale standaardenorganisaties) beschikbaar komen, dient de leverancier binnen een redelijke termijn een migratiepad aan te bieden en te implementeren waarmee de gebruikte encryptie wordt overgezet naar deze quantum-resistente standaard, zonder verlies van functionaliteit of beveiligingsniveau.

TLS-certificaten

Eis 28. TLS-certificaten die worden gebruikt moeten afkomstig zijn van een door het Opdrachtgever goedgekeurde Certificate Authority (CA) en deze moeten automatisch worden vernieuwd minimaal 14 dagen vóór hun vervaldatum.

Verplicht gebruik van cryptografie

Eis 29. Opdrachtnemer moet ervoor zorgen dat alle door hem geleverde diensten, systemen en werkplekken alle gegevens conform het beleidsdocument "Standaard Cryptografie" van Opdrachtgever versleuteld moet worden.

Versleuteling data at rest

Eis 30. Alle opslagmedia van de werkplek, inclusief interne harde schijven en extern verbonden opslagmedia (zoals USB-sticks of externe drives) moeten volledig versleuteld zijn. (Volgens “Standaard Cryptografie”)

Versleuteling van datatransport

Eis 31. Alle communicatie van en naar systemen van de werkplekaanbesteding of andere geleverde systemen moet conform de vertrouwelijkheidsclassificatie worden versleuteld, zodat gegevens tijdens transport beschermd zijn tegen ongeautoriseerde toegang.

Monitoring cryptografie

Eis 32. Opdrachtnemer dient de correcte toepassing van cryptografische maatregelen continu te monitoren.

2.4 Hardening

Configuratie & hardening

Eis 33. Opdrachtnemer is verplicht om op alle door hem beheerde werkplekken, servers en endpoints te hardenen conform het Opdrachtgeverbeleid Regel Veilige Basisconfiguraties (https://beleidshuis-productie.cfapps.eu10.hana.ondemand.com/p/beleidsdocument/28710447625063577) en voert in overleg met Opdrachtgever correcties uit bij afwijkingen.

Policy-gedreven hardening

Eis 34. Opdrachtnemer dient hardening-richtlijnen technisch implementeren als centrale policies.

2.5 ITSM

Authenticatie & Autorisatie

Eis 35. De ITSM-koppeling tussen Opdrachtnemer en Opdrachtgever moet uitsluitend gebruikmaken van moderne authenticatiemechanismen conform het beleid van Opdrachtgever.

Encryptie van dataverkeer

Eis 36. De ITSM-koppeling tussen Opdrachtnemer en Opdrachtgever moet verplicht gebruikmaken van een versleutelde verbinding conform het beleid van Opdrachtgever. Op moment van schrijven is dat TLS 1.2 of hoger met de geadviseerde ciphers van het NCSC.

Koppeling

Eis 37. De ITSM-koppeling tussen Opdrachtnemer en Opdrachtgever wordt op basis van de architectuur richtlijnen van Opdrachtgever opgezet. Op dit moment betekent dit een push/push mechanisme.

RBAC

Eis 38. Opdrachtnemer moet autorisaties implementeren op basis van het principe van ‘least privilege’, zodat elk account, systeem of endpoint alleen toegang heeft tot de minimaal noodzakelijke data en functionaliteiten.

2.6 Key Controls

Gescheiden OTAP-omgevingen

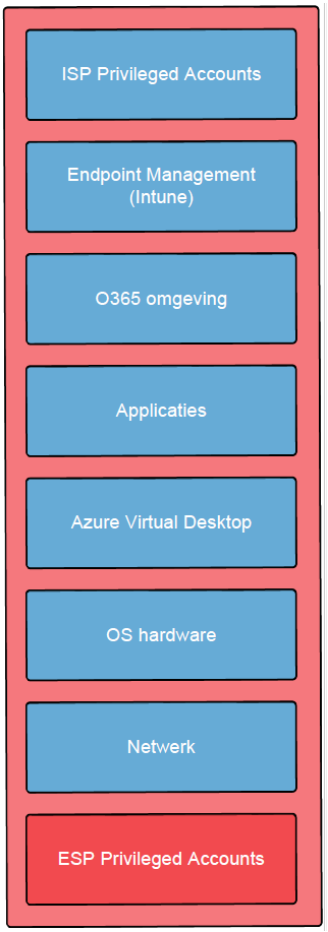
Eis 39. Alle Ontwikkel-, Test-, Acceptatie- en Productieomgevingen dienen op netwerk- en systeemniveau fysiek of logisch gescheiden te worden. Indien afgeweken wordt van deze logische scheiding, zal Opdrachtnemer dit met Opdrachtgever overeenkomen.

2.7 Monitoring & Logging

Aanlevering Security meldingen & audit logs

Eis 40. Opdrachtnemer levert real time geselecteerde security meldingen en (audit) logs aan het SIEM en ondersteunt waar nodig bij de integratie met MSS en de SOC van Opdrachtgever.

Zie Figuur 1: Rood is wat Opdrachtnemer moet monitoren, blauw is wat Opdrachtgever zelf doet.



Figuur 1

Beperkingen aan logging

Eis 41. In een logregel worden in geen geval gevoelige gegevens opgenomen. Dit betreft onder meer gegevens waarmee de beveiliging doorbroken kan worden, waaronder wachtwoorden, inbelnummers, inlogtokens en inlogsessiesleutels. In de logregel mogen ook geen persoonsgegevens worden opgenomen uit systemen van Opdrachtgever zelf (dus wel gebruikersnamen of inlog accounts)

Bescherming van logbestanden

Eis 42. Logfaciliteiten en informatie in logbestanden moeten worden beschermd tegen vervalsing en onbevoegde toegang.

Integratie Opdrachtgever SIEM

Eis 43. Opdrachtnemer mag loggegevens van systemen, werkplekken of applicaties alleen doorsturen via transportmethoden die expliciet door het Opdrachtgever zijn goedgekeurd.

Integratie Kadaster SOC

Eis 44. Opdrachtnemer geeft real-time leestoegang aan het Kadaster SOC en de MSS tot alle relevante (security) configuraties & (audit) logs van de alle fysieke & virtuele apparaten, systemen, softwareplatformen en applicaties die onderdeel zijn van de dienstverlening aan het Kadaster. Het Kadaster en de MSS partij hebben te allen tijde het recht en de bevoegdheid aanvullende informatie op te vragen voor nader onderzoek en/of forensische analyse.

Kloksynchronisatie

Eis 45. De klokken van alle relevante informatie verwerkende systemen moeten worden gesynchroniseerd met de door Opdrachtgever vooraf overeen gekomen NTP-server.

Logbestanden beheeractiviteiten

Eis 46. Opdrachtnemer moet Logbestanden van beheerders en operators, en activiteiten van systeembeheerders en -operators beschermd vastleggen zodat Opdrachtgever die periodiek kan beoordelen.

Logging

Eis 47. Opdrachtnemer zorgt ervoor dat op alle door hem beheerde systemen zodanig worden geconfigureerd dat voor security relevante beveiligings- en systeemevents worden gelogd.

Logregels

Eis 48. Logregels moeten conformeren aan de eisen van Opdrachtgever. Een logregel bevat minimaal:

a. De gebeurtenis;
b. De benodigde informatie die nodig is om het incident met hoge mate van zekerheid te herleiden tot een natuurlijk persoon (de gebruiker zelf)
c. Het gebruikte apparaat, waaronder, Host naam, Operating System (OS)
d. Een datum en tijdstip van de gebeurtenis
e. Waar mogelijk de identiteit van het werkstation of de locatie
f. Naam van de toepassing

g. IP-adres(sen)
h. Het object waarop de handeling werd uitgevoerd
i. Het resultaat van de handeling.

Opslag logging

Eis 49. Opdrachtnemer mag uitsluitend loggegevens die expliciet door Opdrachtgever zijn goedgekeurd doorsturen naar de SIEM omgeving van Opdrachtgever.

Rapportages

Eis 50. Opdrachtnemer levert security rapportages aan Opdrachtgever. De wensen en eisen voor deze rapportages worden in overleg met de securityteams van Opdrachtgever opgesteld.

2.8 Processen

Risicomanagement

Eis 51. Opdrachtnemer heeft een aantoonbaar effectief risicomanagementproces t.a.v. alle aspecten (mens, processen & techniek) die bijdragen aan van de dienstverlening aan Opdrachtgever.

Samenwerking ISP & ESP's

Eis 52. Service Providers zullen voortdurend de samenwerking met andere service providers zoeken bij het afhandelen van een incident, problem, service request, vraag of klacht van de afnemers van de IT-services. Dat houdt concreet in dat Service Providers als eerste op zoek gaan naar een manier om samen iets af te handelen voordat ze zich beroepen op formele afspraken en verantwoordelijkheden. De Service Integrator van Opdrachtgever bewaakt deze afhandeling en zal operationele aanwijzingen geven als dit nodig is om tot een tijdige en correcte afhandeling te komen.

Eis 53. Een technische securityoplossing die over meerdere Leveranciers geleverd moet worden zal door Opdrachtnemer worden geleverd en functioneel beheerd worden (een en ander in samenspraak met Opdrachtgever en de andere Leveranciers) Technische implementatie gebeurt door de verantwoordelijke Leveranciers. Van iedere Leverancier wordt verwacht dat zij indien nodig meewerken bij de implementatie van de gekozen oplossing.

Samenwerking met Kadaster SOC

Eis 54. Opdrachtnemer werkt actief samen met Opdrachtgever bij de afhandeling van security-incidenten die de door opdrachtnemer beheerde systemen betreffen.
Dit houdt in dat Opdrachtnemer:
a. Opdrachtnemer heeft 24/7 gekwalificeerde resources beschikbaar voor het ondersteunen van kritieke security incidenten.
b. Meldingen en opdrachten van het SOC opvolgt binnen afgesproken tijdspanne, afhankelijk van de classificatie van het incident.
c. De gevraagde herstelacties uitvoert, zoals het herinstalleren van werkplekken.
d. De voortgang terugkoppelt aan het SOC volgens de afgesproken communicatielijnen.

Security incidenten

Eis 55. Opdrachtnemer laat eigen interne security incidentprocessen aantoonbaar aansluiten op de security incidentprocessen van Opdrachtgever.

Eis 56. Binnen het Incident Management vormen Security Incidenten een aparte categorie. Net als alle Service Providers moet Opdrachtnemer een maximale inspanning leveren conform de afgesproken normtijden om zo incidenten op te lossen.

Security in de technologie stack t.b.v. MSS

Eis 57. Samen met de MSS partij wordt uiteindelijk door de CISO van Opdrachtgever & de Product Owner bepaalt welke securityoplossing(en) gekozen en geïmplementeerd dient te worden. Dit kan dus ook expliciet een andere securityoplossing zijn van een andere partij. Opdrachtnemer moet meewerken aan de technische implementatie en -integratie met de MSS en het SOC van Opdrachtgever. Opdrachtnemer dient tenminste te waarborgen dat ingezette securityoplossingen integraal aansluiten op het centrale security- en governancelandschap van Opdrachtgever.

Uitvoering van herstelmaatregelen

Eis 58. Opdrachtnemer is verantwoordelijk voor de uitvoering van technische herstelmaatregelen die voortkomen uit security-incidenten of SOC-instructies.
Voorbeelden van herstelacties zijn onder andere:
a. Het herinstalleren of vervangen van gecompromitteerde werkplekken of mobiele apparaten.
b. Het ondersteunen bij het verzamelen van forensische data onder regie van het SOC van Opdrachtgever.

2.9 Vulnerability Management

Beheer

Eis 59. Opdrachtnemer is verantwoordelijk voor het dagelijks beheer van de scanning software. Hieronder valt: implementatie van updates en policy-wijzigingen, oplossen van foutmeldingen en agentproblemen, zorgen dat agents actief blijven en up-to-date zijn.

Gezamenlijke prioritering

Eis 60. Opdrachtnemer levert input en advies over de technische impact, uitvoerbaarheid en afhankelijkheden, zodat Opdrachtgever een weloverwogen prioriteit kan vaststellen. De prioriteit indeling is vastgelegd in de "Licence to Operate" van Opdrachtgever.

Mitigeren kwetsbaarheden

Eis 61. Opdrachtnemer moet mitigerende maatregels implementeren binnen de door Opdrachtgever vastgestelde termijnen zoals beschreven in het beleid van Opdrachtgever. De prioriteit indeling is vastgelegd in de "Licence to Operate" van Opdrachtgever.

Ondersteuning bij mitigatie

Eis 62. Opdrachtnemer moet actief ondersteunen bij het uitvoeren van mitigerende maatregelen, zoals: het aanpassen van configuraties, toepassen van firewallregels, beperken van toegang, of het tijdelijk isoleren van systemen.

Patchvalidatie en controle

Eis 63. Na installatie van patches moet Opdrachtnemer verifiëren dat de kwetsbaarheid daadwerkelijk is opgelost en dat er geen negatieve impact is op functionaliteit.

Respons binnen prioriteringsproces

Eis 64. Opdrachtnemer moet binnen afgesproken tijden reageren op verzoeken van Opdrachtgever met technische onderbouwing of advies over prioriteit en risico van een kwetsbaarheid.

3. Monitoring & Control

3.1 Hardening

Monitoring

Eis 65. Opdrachtnemer moet voorzien in een mechanisme voor continue monitoring van de naleving van de hardening-configuraties, zodat afwijkingen automatisch worden gedetecteerd en gerapporteerd.

3.2 Pentest

Oplossen bevindingen

Eis 66. Opdrachtnemer geeft medewerking aan het nemen van eventuele mitigerende maatregelen die uit de A&P test kunnen voortvloeien.

Pentesten

Eis 67. Opdrachtgever heeft het recht om een A&P-test uit te voeren:
a. Als onderdeel van de Acceptatietest voor in-productie-name van de Oplossing
b. Minimaal één keer per jaar
c. Bij iedere grote wijziging van de Oplossing

3.3 Right to audit

Audit recht/security onderzoeken

Eis 68. Opdrachtgever kan een risicoanalyse of externe audit, waaronder een penetratietest, laten uitvoeren om te controleren of aan beveiligingseisen die van toepassing zijn wordt voldaan. Een audit is niet nodig als Opdrachtnemer aantoont dat er al een recente (binnen 1 jaar) onafhankelijke audit heeft plaatsgevonden op de gewenste scope en de relevante resultaten deelt met Opdrachtgever. Als Opdrachtnemer niet kan of niet wenst te voldoen aan de gestelde bevindingen uit een audit, heeft Opdrachtgever de mogelijkheid tot opzeggen van de te sluiten overeenkomst.

3.4 Vulnerability Management

Monitoring van status en gezondheid

Eis 69. Opdrachtnemer moet continu monitoren of de tooling actief is op alle apparaten, en afwijkingen (zoals uitgeschakelde agents of ontbrekende updates) binnen 24 uur corrigeren of melden aan het Opdrachtgever.

Vulnerabilityscanning

Eis 70. Opdrachtnemer voert periodiek (minimaal elke week) een technische vulnerability scan uit op alle fysieke & virtuele apparaten, systemen, softwareplatformen en applicaties die onderdeel zijn van de dienstverlening aan Opdrachtgever en voert hier zelf proactief vulnerability management op uit. (risicogebaseerde aanpak)
De resultaten van de technische vulnerability scan worden door Opdrachtnemer geautomatiseerd bijgewerkt in het Security Operations platform van Opdrachtgever.