Bijlage 22a IB-eisen

Digitale werkplek (DWP) perceel 1
Werkplekservices
Kadaster

Directie Governance, Data en Vernieuwing

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

IB-eisen Werkplekservices

1. Automation & Orchestration

1.1 Connectivity

Network Access Control

Eis 1. De Opdrachtnemer dient ervoor te zorgen dat de configuratiebestanden van de door de 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. De 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.

Eis 3. De Opdrachtnemer dient ervoor te zorgen dat de configuratiebestanden van de door het Opdrachtgever aangewezen Connectivity leverancier, inclusief instellingen, op alle door hem beheerde werkplekken correct worden toegepast, geconfigureerd en up-to-date gehouden.

1.2 Patch- & Lifecyclemanagement

Opdrachtnemersketen

Eis 4. Indien de 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 5. De Opdrachtnemer moet een geautomatiseerd patchmanagementproces toepassen waarmee updates kunnen worden uitgerold, getest en gemonitord, inclusief logging van installatiestatus.

Afwijkingsprocedure bij incompatibiliteit

Eis 6. Indien een patch niet geïnstalleerd kan worden, moet de Opdrachtnemer dit binnen 24 uur melden aan het Opdrachtgever, met een onderbouwde risicoanalyse en herstelplan.

Herijking hardware levensduur

Eis 7. *Uitvoeringseis* - De 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 8. 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 de Opdrachtgever.

Eis 9. Indien een patch niet binnen de afgesproken termijn kan worden geïmplementeerd, moet de 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 10. Nieuwe software- en beveiligingsupdates moeten conform het beleid "License to Operate" van de 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 11. De 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 de opdrachtgever met betrekking tot de producten die vallen onder deze aanbesteding en zo binnen gestelde SLA-tijden van de security patches worden voorzien conform het beleid "License to Operate" van de Opdrachtgever.

Eis 12. De Opdrachtnemer voert volgende type updates uit die buiten het beleid "License to Operate" van de 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 13. De 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 "License to Operate" van de Opdrachtgever..

Virusdefinities

Eis 14. Opdrachtnemer moet alle anti-malwareoplossingen minimaal dagelijks moeten monitoren en indien nodig bijwerken met de nieuwste malwaredefinities.

1.3 Vulnerability Management

Vulnerabilityscanning

Eis 15. De Opdrachtnemer moet op alle door hem beheerde werkplekken en mobiele apparaten de kwetsbaarheden scanner van de Opdrachtgever installeren en correct configureren.

Eis 16. De Opdrachtnemer moet de tooling volgens de minimale beveiligingsinstellingen die door Opdrachtgever zijn vastgesteld configureren.

Verwerking bevindingen

Eis 17. De 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 18. *Uitvoeringseis* - De 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 19. *Uitvoeringseis* - De 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 20. *Uitvoeringseis* - De 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 21. De 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 22. 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 23. De Opdrachtnemer moet ervoor zorgen dat de data in de CMDB consistent is met andere relevante bronnen (zoals bijvoorbeeld Microsoft Intune)

Datakwaliteit & actualiteit

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

Integratie & samenwerking

Eis 25. De Opdrachtnemer moet de CMDB van de 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 26. Iedere geregistreerde asset moet voorzien zijn van een uniek identificatienummer (bijv. Asset-ID of Configuration Item-ID) dat correspondeert met de Opdrachtgever-standaard voor assetnaming.

2.3 Encryptie

Implementatie en Beheer

Eis 27. De Opdrachtnemer is verantwoordelijk voor het correct implementeren, beheren en monitoren van alle cryptografische maatregelen op alle relevante systemen en diensten.

Quantum-resistente encryptie

Eis 28. 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 29. 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 30. De Opdrachtnemer moet ervoor zorgen dat alle door hem geleverde diensten, systemen en werkplekken alle gegevens conform het beleidsdocument "Standaard Cryptografie" van de Opdrachtgever versleuteld moet worden.

Versleuteling data at rest

Eis 31. 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 32. 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 33. De Opdrachtnemer dient de correcte toepassing van cryptografische maatregelen continu te monitoren.

2.4 Hardening

Configuratie & hardening

Eis 34. De 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 35. De Opdrachtnemer dient hardening-richtlijnen technisch implementeren als centrale policies.

2.5 Informatie beveiliging

Classificatie

Eis 36. Alle vormen van informatie moet conform afgesproken veiligheids classificering kunnen worden ingedeeld. De classificering wordt in overleg met Opdrachtgever afgestemd. De Opdrachtgever is hierin leidend.

Eis 37. De classificering van informatie moet zoveel mogelijk automatisch kunnen gebeuren. Bijvoorbeeld op basis van meta informatie, met behulp van automatiseerbare rules. De methode en automatisering daarvan moeten in samenspraak met Opdrachtgever bepaald worden. De Opdrachtgever is hierin leidend.

Eis 38. Onjuist geclassificeerde informatie kan een (veiligheids)risico vormen. Opdrachtnemer moet medewerking verlenen bij de mitigatie van dergelijke risico's. Dit omvat ook het opruimen van gevolgen van de onjuiste classificatie.

Eis 39. Opdrachtnemer zal periodiek rapporteren op alle ingestelde classificaties en acties (automatiseerbare rules) die daaraan hangen. De periode van rapportage zal in samenspraak met Opdrachtgever worden bepaald. De Opdrachtgever is hierin leidend.

Eis 40. Aan alle classificaties hangen veiligheidseisen en veiligheidsrisico's. Deze eisen en risico's worden in overleg met opdrachtgever afgestemd.

Eis 41. Opdrachtnemer voert risico mitigerende maatregelen uit voor niet-acceptabele risico's in samenspraak met opdrachtgever en op verzoek van opdrachtgever ook met andere serviceproviders. Bijvoorbeeld het blokkeren van email of email in quarantaine plaatsen

Eis 42. Opdrachtnemer dient alle AI toepassingen binnen een veiligheids classificatie te plaatsen en deze af te stemmen met de Opdrachtgever.

2.6 ITSM

Authenticatie & Autorisatie

Eis 43. De ITSM-koppeling tussen de Opdrachtnemer en Opdrachtgever moet uitsluitend gebruikmaken van moderne authenticatiemechanismen conform het beleid van de Opdrachtgever.

Encryptie van dataverkeer

Eis 44. De ITSM-koppeling tussen de Opdrachtnemer en Opdrachtgever moet verplicht gebruikmaken van een versleutelde verbinding conform het beleid ” Bijlage 24 License to Operate 1.0” van de Opdrachtgever. Op moment van schrijven is dat TLS 1.2 of hoger met de geadviseerde ciphers van het NCSC.

Koppeling

Eis 45. De ITSM-koppeling tussen de Opdrachtnemer en Opdrachtgever wordt op basis van de architectuur richtlijnen van de Opdrachtgever opgezet. Op dit moment betekent dit een push/push mechanisme.

RBAC

Eis 46. De 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.

2.7 Key Controls

Gescheiden OTAP-omgevingen

Eis 47. 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 de Opdrachtnemer dit met de Opdrachtgever overeenkomen.

2.8 Mail & Messaging

Classificatie

Eis 48. Alle inkomende en uitgaande email en messaging moet conform afgesproken veiligheids classificering kunnen worden ingedeeld. De classificering wordt in overleg met Opdrachtgever afgestemd.

Eis 49. Alle bijgevoegde bestanden en documenten in inkomende en uitgaande mail en messaging moeten conform afgesproken classificatie worden ingedeeld. De classificering wordt in overleg met Opdrachtgever afgestemd.

Continuïteit en compliance

Eis 50. De Opdrachtnemer moet garanderen dat alle TLS-certificaten automatisch worden vernieuwd en afkomstig zijn van een door het Opdrachtgever goedgekeurde Certificate Authority (CA).

E-mail beveiliging

Eis 51. Opdrachtnemer rapporteert direct aan Opdrachtgever bij signalering van risicovolle activiteiten

Eis 52. Opdrachtnemer evalueert in samenspraak met opdrachtgever periodiek alle risico mitigerende maatregelen en komt met adviezen voor verbeteringen. De periode moet in samenspraak met Opdrachtgever worden vastgesteld.

Eis 53. Bij beveiligingsincidenten is de Opdrachtnemer beschikbaar en ondersteunt Opdrachtnemer het komen tot een voor Opdrachtgever acceptabele oplossing.

Training en Simulatie

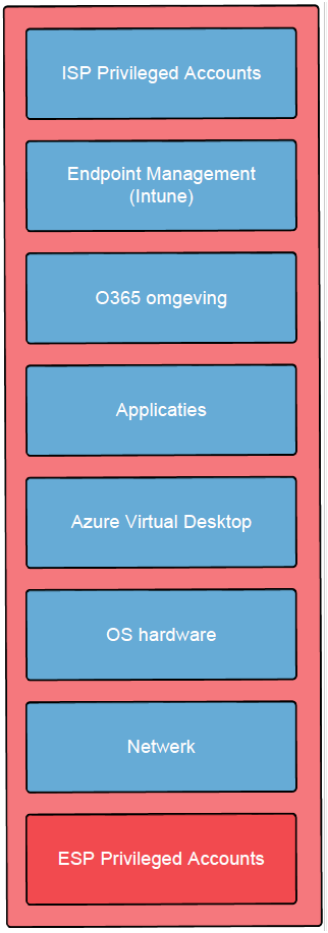
Eis 54. De Opdrachtnemer faciliteert op verzoek van Opdrachtgever bij trainingen en/of simulaties ten behoeve van een veiliger gebruik van email en alle facetten daarvan. Denk bijvoorbeeld aan phishing simulaties en algemene trainingen.

2.9 Monitoring & Logging

Aanlevering Security meldingen & audit logs

Eis 55. De 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 de Opdrachtnemer moet monitoren, blauw is wat Opdrachtgever zelf doet.



Figuur 1

Beperkingen aan logging

Eis 56. 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 de opdrachtgever zelf (dus wel gebruikersnamen of inlog accounts)

Bescherming van logbestanden

Eis 57. Logfaciliteiten en informatie in logbestanden moeten worden beschermd tegen vervalsing en onbevoegde toegang.

Integratie Opdrachtgever SIEM

Eis 58. De Opdrachtnemer mag loggegevens van systemen, werkplekken of applicaties alleen doorsturen via transportmethoden die expliciet door het Opdrachtgever zijn goedgekeurd.

Integratie Kadaster SOC

Eis 59. De 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 60. De klokken van alle relevante informatie verwerkende systemen moeten worden gesynchroniseerd met de door de Opdrachtgever vooraf overeengekomen NTP-server.

Logbestanden beheeractiviteiten

Eis 61. De Opdrachtnemer moet Logbestanden van beheerders en operators, en activiteiten van systeembeheerders en -operators beschermd vastleggen zodat de Opdrachtgever die periodiek kan beoordelen.

Logging

Eis 62. De Opdrachtnemer zorgt ervoor dat op alle door hem beheerde systemen zodanig worden geconfigureerd dat voor security relevante beveiligings- en systeemevents worden gelogd.

Logregels

Eis 63. 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 64. De Opdrachtnemer mag uitsluitend loggegevens die expliciet door de Opdrachtgever zijn goedgekeurd doorsturen naar de SIEM omgeving van de Opdrachtgever.

Rapportages

Eis 65. De Opdrachtnemer levert security rapportages aan de Opdrachtgever. De wensen en eisen voor deze rapportages worden in overleg met de securityteams van de Opdrachtgever opgesteld.

2.10 Processen

"Noodknop mandaat" afspraken

Eis 66. De Opdrachtnemer werkt mee aan de implementatie en het mogelijk deels geautomatiseerd toepassen van het SOC/MSS 'noodknop' mandaat van Opdrachtgever. Dit om bepaalde onderdelen (tijdelijk) te isoleren en/of uit te schakelen, om de schade van een security incident te helpen beperken.

Risicomanagement

Eis 67. De 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 68. 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 69. 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 70. De Opdrachtnemer werkt actief samen met de Opdrachtgever bij de afhandeling van security-incidenten die de door opdrachtnemer beheerde systemen betreffen.
Dit houdt in dat de Opdrachtnemer:

a. De 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 71. De Opdrachtnemer laat eigen interne security incidentprocessen aantoonbaar aansluiten op de security incidentprocessen van Opdrachtgever.

Eis 72. 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 73. 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. De Opdrachtnemer moet meewerken aan de technische implementatie en -integratie met de MSS en het SOC van Opdrachtgever. De Opdrachtnemer dient tenminste te waarborgen dat ingezette securityoplossingen integraal aansluiten op het centrale security- en governancelandschap van Opdrachtgever.

Uitvoering van herstelmaatregelen

Eis 74. De 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 de Opdrachtgever.

2.11 Vulnerability Management

Beheer

Eis 75. De 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 76. De 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 77. De Opdrachtnemer moet mitigerende maatregels implementeren binnen de door Opdrachtgever vastgestelde termijnen zoals beschreven in het beleid van de Opdrachtgever. De prioriteit indeling is vastgelegd in de "Licence to Operate" van Opdrachtgever.

Ondersteuning bij mitigatie

Eis 78. De 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 79. Na installatie van patches moet de Opdrachtnemer verifiëren dat de kwetsbaarheid daadwerkelijk is opgelost en dat er geen negatieve impact is op functionaliteit.

Respons binnen prioriteringsproces

Eis 80. De Opdrachtnemer moet binnen afgesproken tijden reageren op verzoeken van Opdrachtgever met technische onderbouwing of advies over prioriteit en risico van een kwetsbaarheid.

2.12 Werkplek

Endpoint Privilege Management Licentiebeheer

Eis 81. De Opdrachtnemer beheert uitsluitend de door de Opdrachtgever verstrekte licenties voor EPM-software en garandeert dat het gebruik volledig in lijn is met de Opdrachtgeverlicenties en voorwaarden.

URL Filtering

Eis 82. De Opdrachtnemer dient ervoor te zorgen dat de benodigde software van de door de Opdrachtgever aangewezen Connectivity Leverancier op alle door hem beheerde werkplekken en mobiele apparaten correct worden geïnstalleerd, geconfigureerd, bijgewerkt en operationeel gehouden, zodat de URL-filtering correct functioneren volgens het Opdrachtgeverbeleid.

2.13 Werkplek + Mobiele Telefoon

EDR Licentiebeheer

Eis 83. De Opdrachtnemer beheert uitsluitend de door het Opdrachtgever verstrekte licenties voor EDR/AV-software en garandeert dat het gebruik volledig in lijn is met de Opdrachtgeverlicenties en voorwaarden.

3. Monitoring & Control

3.1 Collaboration Space

Beveiliging van Samenwerkingsplatforms

Eis 84. De Opdrachtnemer is verantwoordelijk voor de configuratie, het beheer en de instandhouding van de bestaande oplossing van de Opdrachtgever ten behoeve van beveiliging binnen de samenwerkingsplatforms.

a. De Opdrachtnemer dient de oplossing zodanig te configureren dat de samenwerkingsplatforms beschikken over geïntegreerde anti-malwarefunctionaliteit die alle geüploade en gedownloade bestanden automatisch controleert op kwaadaardige code.
b. De oplossing moet alle URL's in Teams-chats, gedeelde documenten en bestandsbeschrijvingen automatisch analyseren op potentiële schadelijkheid. Indien een link als kwaadaardig wordt aangemerkt, moet toegang tot de link worden geblokkeerd of een waarschuwing aan de gebruiker worden getoond.

Monitoring

Eis 85. De Opdrachtgever moet rapporteren op de huidige gebruikers van de Microsoft 365 Tenant. Bijvoorbeeld het kunnen filteren op externe domeinen binnen de gebruikers inlog gegevens.

3.2 Hardening

Monitoring

Eis 86. De Opdrachtnemer moet voorzien in een mechanisme voor continue monitoring van de naleving van de hardening-configuraties, zodat afwijkingen automatisch worden gedetecteerd en gerapporteerd.

3.3 Mail & Messaging

E-mail beveiliging

Eis 87. Alle inkomende en uitgaande emailverkeer moeten door de Opdrachtnemer gecontroleerd en gemonitord worden op veiligheidsrisico's en risicovolle activiteiten. Deze risico's worden in overleg met Opdrachtgever afgestemd. Opdrachtgever is hierin leidend. Bijvoorbeeld emails scannen op malware, op phishing en spam en/of op URL's en die analyseren. Maar ook het detecteren van pogingen tot inbraak door kwaadwillenden.

Eis 88. Alle inkomende en uitgaande emailverkeer moeten door de Opdrachtnemer aan de hand van whitelisting kunnen worden vrijgesteld van risicomitigatie. Deze whitelist wordt door Opdrachtgever bijgehouden.

Ondersteuning Connectivity

Eis 89. Al het inkomend en uitgaand emailverkeer dient volgens afgesproken methoden te worden beveiligd en geauthentiseerd. Deze methoden worden in overleg met Opdrachtgever afgestemd. Opdrachtgever is hierin leidend. Bijvoorbeeld SPF, DKIM, DMARC, DANE.

Eis 90. Opdrachtnemer draagt zorg voor de correcte werking van alle afgesproken methoden en werkt daarin samen met Opdrachtgever en op verzoek van Opdrachtgever ook met andere serviceproviders. Bijvoorbeeld het configureren van DNS records wat door de leverancier van het Connectivity kavel wordt uitgevoerd.

Transportversleuteling (TLS/Secure Mail)

Eis 91. Het transport van alle inkomende en uitgaande emailverkeer moet versleuteld zijn met een van de door Opdrachtgever aangedragen acceptabele methodieken. Deze methodieken worden in overleg met Opdrachtgever afgestemd. Als inkomend of uitgaand emailverkeer hier niet aan voldoet moet het emailverkeer door de Opdrachtnemer worden geweigerd en de verzender op de hoogte worden gesteld aan de hand van een foutmelding.

3.4 Pentest

Oplossen bevindingen

Eis 92. Opdrachtnemer geeft medewerking aan het nemen van eventuele mitigerende maatregelen die uit de A&P test kunnen voortvloeien.

Pentesten

Eis 93. 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

3.5 Right to audit

Audit recht/security onderzoeken

Eis 94. 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 de 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 de Opdrachtnemer niet kan of niet wenst te voldoen aan de gestelde bevindingen uit een audit, heeft de Opdrachtgever de mogelijkheid tot opzeggen van de te sluiten overeenkomst.

3.6 Vulnerability Management

Monitoring van status en gezondheid

Eis 95. De 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 96. De 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.

3.7 Werkplek

Endpoint Privilege Management

Eis 97. De Opdrachtnemer is verplicht om op alle door hem beheerde werkplekken binnen de opdracht de door het Opdrachtgever voorgeschreven Endpoints Privilege Management (EPM) client-software te installeren, configureren, beheren en up-to-date houden, conform de beveiligingsrichtlijnen van het Opdrachtgever. Belangrijk: Licenties worden door de Opdrachtgever verzorgd.

3.8 Werkplek + Mobiele Telefoon

Implementatie biometrie op apparaten

Eis 98. De Opdrachtnemer dient ervoor te zorgen dat op alle door hem beheerde fysieke werkplekken en mobiele apparaten de door het Opdrachtgever voorgeschreven biometrische authenticatie (zoals vingerafdruk of gezichtsherkenning) wordt ondersteund.

Installatie en beheer antivirus- en EDR-software

Eis 99. De Opdrachtnemer is verplicht om op alle door hem beheerde werkplekken, servers en endpoints binnen de opdracht de door het Opdrachtgever voorgeschreven antivirus- en Endpoint Detection & Response (EDR)-software te installeren, configureren, beheren en up-to-date houden, conform de

beveiligingsrichtlijnen van het Opdrachtgever. Belangrijk: Licenties en incidentrespons worden door de Opdrachtgever verzorgd.

Opslag Biometrische gegevens

Eis 100. Biometrische gegevens worden uitsluitend lokaal verwerkt binnen een beveiligde hardware-omgeving (bijvoorbeeld TPM of Secure Enclave). Alleen de cryptografisch beveiligde verificatie van de gebruiker wordt gedeeld met systemen of applicaties; ruwe biometrische gegevens worden nooit opgeslagen of uitgewisseld.

Toekomstbestendig passwordless framework

Eis 101. De Opdrachtnemer draagt zorg voor een toekomstbestendige inrichting van het authenticatie framework, waarbij de biometrische infrastructuur compatibel is met passwordless authenticatie op basis van cryptografische sleutels, zodat traditionele wachtwoorden in de toekomst volledig vervangen kunnen worden.