

Bijlage 17

Informatiebeveiliging VOR-IN

Gemeente Amsterdam

Opdrachtgever:	Verkeer & Openbare Ruimte Gemeente Amsterdam
Contractnummer:	AI 2021-0047
Versie:	1.0
Datum:	15-06-2021

Inhoudsopgave

1	Over dit document.....	3
2	Inleiding	4
3	Baselinetoets IDMA	5
4	Maatregelen.....	6

1 Over dit document

De Baseline Informatiebeveiliging Overheden (BIO) vormt het normenkader voor de informatiebeveiliging bij de overheid. De meest recente versie van de BIO is beschikbaar op: <https://bio-overheid.nl/>

De BIO beschrijft de invulling van de NEN-ISO/IEC 27001:2017 en de NEN-ISO/IEC 27002:2017 voor de overheid. De NEN-ISO/IEC 27001:2017 en de NEN-ISO/IEC 27002:2017 beschrijven de details voor implementatie (implementatierichtlijnen) en eisen voor de procesinrichting en geven dus de details voor de toepassing, die niet in de BIO zijn beschreven en die nodig blijven voor een goede implementatie van de BIO.

Te allen tijde blijven de NEN-ISO/IEC 27001:2017 en de NEN-ISO/IEC 27002:2017 leidend. De uitwerkingen die in dit document zijn opgenomen, bieden de Leverancier relevante informatie over de wijze waarop de gemeente Amsterdam - en specifiek hoe binnen de eenheid V&OR, Afdeling Stedelijk Beheer, Team Licht - invulling geeft aan de informatiebeveiliging op de systemen, informatie en processen binnen het VOR-IN. Deze invulling heeft directe gevolgen voor de controls uit NEN-ISO/IEC 27002 die de Leverancier dient te implementeren.

Informatiebeveiliging is geen eenmalige activiteit, maar vergt een repeterend proces van evalueren en bijstellen. De maatregelen en controles kunnen dan ook wijzigen in de loop der tijd, om te blijven voldoen aan de baseline en BIO om het hoofd te kunnen bieden aan de informatiebeveiligingsrisico's.

Daarbij is en blijft het 'pas toe of leg uit' principe van toepassing. Voor de diverse toe te passen standaarden wordt nadrukkelijk verwezen naar het Forum Standaardisatie: <https://www.forumstandaardisatie.nl/>

NEN-ISO/IEC 27001:2017 en de NEN-ISO/IEC 27002:2017 gaan boven de BIO en de BIO gaat boven dit document. Discrepancies tussen dit document en het Programma van Eisen worden in overleg met (een vertegenwoordiger van) de CISO van Amsterdam besproken.

2 Inleiding

Informatiebeveiliging is gericht op bescherming van informatie. Deze bescherming maakt het mogelijk om elektronische dienstverlening en gegevensuitwisseling op een verantwoorde wijze uit te voeren. Het doel van informatiebeveiliging is het waarborgen van:

- De beschikbaarheid van gegevens en systemen (zijn de gegevens continue beschikbaar);
- De integriteit van gegevens (zijn de gegevens juist, actueel en volledig);
- De vertrouwelijkheid van gegevens (zijn de gegevens alleen beschikbaar voor bevoegden).

De BIO definieert de volgende veertien categorieën van beveiligingsmaatregelen die noodzakelijk worden geacht om te kunnen voldoen aan het principe van "goed huisvaderschap", te weten (de nummers komen overeen met de hoofdstukken uit de BIO):

5. Informatiebeveiligingsbeleid,
6. Organiseren van informatiebeveiliging,
7. Veilig personeel,
8. Beheer van bedrijfsmiddelen,
9. Toegangsbeveiliging,
10. Cryptografie,
11. Fysieke beveiliging en beveiliging van de omgeving ,
12. Beveiliging bedrijfsvoering
13. Communicatiebeveiliging
14. Acquisitie, ontwikkeling en onderhoud van informatiesystemen,
15. Leveranciersrelaties,
16. Beheer van informatiebeveiligingsincidenten,
17. Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer en
18. Naleving.

3 Baselinetoets IDMA

De maatregelen worden getroffen op basis van een risicoafweging, waarbij de BIO leidend is. Met behulp van een baselinetoets is bepaald of de IDMA een bepaald BasisBeveiligingsNiveau (BBN) heeft binnen de BIO. Uit deze baselinetoets blijkt dat het BBN-niveau 2 van toepassing is op de IDMA, op elk aspect (Beschikbaarheid, Integriteit, Vertrouwelijkheid). Dit houdt in dat alle BBN2 controls uit de BIO uitgewerkt moeten zijn in maatregelen.

Leverancier dient zich te conformeren aan de eisen en uitgangspunten van de gemeente Amsterdam met betrekking tot de subset controls en maatregelen. De uitgangspunten en eisen zijn voor deze subset uitgewerkt in dit document, voor zover dat in een publiek beschikbaar document mogelijk is zonder inbreuk te doen op de informatiebeveiliging.

Aan de hand van de baselinetoets is eveneens vastgesteld of er persoonsgegevens worden verwerkt. Zowel uit de baselinetoets als uit additioneel overleg met een privacy officer van de gemeente Amsterdam blijkt dat er geen sprake is van de verwerking van persoonsgegevens in de huidige scope van (de informatieverwerking door) de IDMA. Doorontwikkeling van de IDMA kan ertoe leiden dat er in de toekomst wel sprake kan zijn van de verwerking van persoonsgegevens. Op het moment van schrijven wordt dit echter niet voorzien.

4 Maatregelen

Onderstaande tabel geeft de nummers uit de BIO weer en bijbehorende Control / Beveiligingsmaatregel. De BIO nummering sluit direct aan op de nummering uit de NEN-ISO/IEC 27001:2017 (Hoofdstuk.paragraaf) en de NEN-ISO/IEC 27002:2017 (Hoofdstuk.paragraaf.beheersmaatregel)

BIO nr.	Control / Beveiligingsmaatregel	Eis / uitgangspunt
5.1.1.1	Er is een informatiebeveiligingsbeleid opgesteld door de organisatie. Dit beleid is vastgesteld door de leiding van de organisatie en bevat tenminste de volgende punten: a) de strategische uitgangspunten en randvoorwaarden die de organisatie hanteert voor informatiebeveiliging en in het bijzonder de inbedding in, en afstemming op het algemene beveiligingsbeleid en het informatievoorzieningsbeleid; b) de organisatie van de informatiebeveiligingsfunctie, waaronder verantwoordelijkheden, taken en bevoegdheden; c) de toewijzing van de verantwoordelijkheden voor ketens van informatiesystemen aan lijnmanagers; d) de gemeenschappelijke betrouwbaarheidseisen en normen die op de organisatie van toepassing zijn; e) de frequentie waarmee het informatiebeveiligingsbeleid wordt geëvalueerd; f) de bevordering van het beveiligingsbewustzijn.	Leverancier toont aan te beschikken over door de directie vastgesteld informatiebeveiligingsbeleid gebaseerd op de ISO 27001 en 27002, die betrekking heeft op de aangeboden dienstverlening. Het informatiebeveiligingsbeleid dient te worden goedgekeurd door de opdrachtnemer, ter beschikking gesteld aan en gecommuniceerd met de opdrachtgever, medewerkers en andere relevante externe partijen.
5.1.2.1	Het informatiebeveiligingsbeleid wordt periodiek en in aansluiting bij de (bestaande) bestuurs- en P&C-cycli en externe ontwikkelingen beoordeeld en zo nodig bijgesteld.	Leverancier toont aan ten minste jaarlijks te beoordelen en bij te stellen.
6.1.1.1	De leiding van de organisatie heeft vastgelegd wat de verantwoordelijkheden en rollen zijn op het gebied van informatiebeveiliging binnen haar organisatie.	Leverancier toont dit aan middels document(en), waarin opgenomen de functionarissen die rollen en verantwoordelijkheden op het gebied van informatiebeveiliging uitvoeren.
6.1.1.2	De verantwoordelijkheden en rollen ten aanzien van informatiebeveiliging zijn gebaseerd op relevante voorschriften en wetten.	Leverancier verklaart het beleid jaarlijks te toetsen op ten minste ISO normen en levert deze toetsing geanonimiseerd aan.
6.1.1.3	De rol en verantwoordelijkheden van de Chief Information Security Officer (CISO) zijn in een CISO-functieprofiel vastgelegd.	Leverancier toont dit aan en levert Opdrachtgever contactgegevens van de CISO aan.
6.1.1.4	Er is een CISO aangesteld conform een vastgesteld CISO-functieprofiel.	Zie 6.1.1.3.

BIO nr.	Control / Beveiligingsmaatregel	Eis / uitgangspunt
6.1.2.1	Er zijn maatregelen getroffen die onbedoelde of ongeautoriseerde toegang tot bedrijfsmiddelen waarnemen of voorkomen.	Leverancier toont met een document aan welke maatregelen zijn genomen met betrekking tot de eigen bedrijfsmiddelen, alsmede met betrekking tot de toegang tot de bedrijfsmiddelen van Amsterdam.
6.1.3.1	Er is door de organisatie uitgewerkt wie met welke (overheids)instanties en toezichthouders contact heeft ten aanzien van informatiebeveiligingsaangelegenheden (vergunningen/incidenten/calamiteiten) en welke eisen voor deze aangelegenheden relevant zijn.	Onderdeel van de SLA en DAP
6.1.3.2	Het contactoverzicht wordt jaarlijks geactualiseerd.	Onderdeel van de DAP.
6.2.1.1	Mobiele apparatuur is zo ingericht dat bedrijfsinformatie niet onbewust wordt opgeslagen ('zero footprint'). Als zero footprint (nog) niet realiseerbaar is, biedt een mobiel apparaat (zoals een laptop, tablet en smartphone) de mogelijkheid om de toegang te beschermen door middel van een toegangsbeveiligingsmechanisme en, indien vertrouwelijke gegevens worden opgeslagen, versleuteling van die gegevens. In het geval van opslag van vertrouwelijke informatie moet op deze mobiele apparatuur 'wissen op afstand' mogelijk zijn.	Leverancier toont dit aan voor alle mobiele apparatuur die toegang biedt tot bedrijfsinformatie van Opdrachtgever en Leverancier.
6.2.1.2	Bij de inzet van mobiele apparatuur zijn minimaal de volgende aspecten geïmplementeerd: a) In bewustwordingsprogramma's komen gedragsaspecten van veilig mobiel werken aan de orde. b) Het device maakt deel uit van patchmanagement en hardening. c) Er wordt gebruik gemaakt van Mobile Device Management MDM of van Mobile Application Management (MAM)-oplossingen. d) Gebruikers tekenen een gebruikersovereenkomst voor mobiel werken, waarmee zij verklaren zich bewust te zijn van de gevaren van mobiel werken en verklaren dit veilig te zullen doen. Deze verklaring heeft betrekking op alle mobiele apparatuur die de medewerker zakelijk gebruikt. e) Periodiek wordt getoetst of de punten in lid b), c) en d) worden nageleefd	Leverancier toont aan dit vastgelegd te hebben in beleid en procedures aangaande het gebruik van mobiele apparatuur en verklaart dat alle betrokken medewerkers hiervan op de hoogte zijn.

BIO nr.	Control / Beveiligingsmaatregel	Eis / uitgangspunt
7.1.1.1	Elke organisatie heeft een vastgesteld screeningsbeleid. Bij indiensttreding en bij functiewijziging kan een Verklaring Omtrent het Gedrag (VOG) gevraagd worden.	Leverancier toont dit aan en levert aan Opdrachtgever van alle medewerkers die werkzaamheden verrichten in het kader van de overeenkomst: Naam, telefoonnummer en getekende geheimhoudingsverklaring. Tevens wordt een VOG geleverd of ter inzage voorgelegd, die niet ouder is dan 1 jaar. De VOG is aangevraagd met de volgende kenmerken: • Werken bij bedrijf of instelling als engineer, projectverantwoordelijke • Algemeen screeningsprofiel op functieaspecten: informatie 11, informatie 12, diensten 41. Aanvullend wordt van elke werknemer die toegang krijgt tot de IDMA of VOR-IN een (zakelijk) persoonlijk e-mailadres en een getekende integriteit- en geheimhoudingsverklaring (I&G) van de gemeente Amsterdam verlangd.
7.1.2.1	Alle medewerkers (intern en extern) zijn bij hun aanstelling of functiewisseling gewezen op hun verantwoordelijkheden ten aanzien van informatiebeveiliging. De voor hen geldende regelingen en instructies ten aanzien van informatiebeveiliging zijn eenvoudig toegankelijk.	Leverancier verklaart dit.
7.2.1.1	Er is aansluiting bij een klokkenluidersregeling, zodat iedereen anoniem en veilig beveiligingsissues kan melden.	Leverancier toont dit aan.
7.2.2.1	Alle medewerkers hebben de verantwoordelijkheid bedrijfsinformatie te beschermen. Iedereen kent de regels en verplichtingen met betrekking tot informatiebeveiliging en daar waar relevant de speciale eisen voor gerubriceerde omgevingen	Leverancier toont aan middels een overzicht dat er scheiding van data is.
7.2.2.2	Alle medewerkers en contractanten die gebruikmaken van de informatiesystemen- en diensten hebben binnen drie maanden na indiensttreding een training I-bewustzijn succesvol gevolgd.	Leverancier toont aan dat nieuwe medewerkers die werkzaamheden verrichten in het kader van de Overeenkomst deze training hebben gevolgd.
7.2.2.3	Het management benadrukt bij aanstelling en interne overplaatsing en bijvoorbeeld in werkoverleggen of in personeelsgesprekken bij zijn medewerkers en contractanten het belang van opleiding en training op het gebied van informatiebeveiliging en stimuleert hen actief deze periodiek te volgen.	Leverancier toont dit aan. De training dient elke 3 jaar opnieuw te worden gevolgd.

BIO nr.	Control / Beveiligingsmaatregel	Eis / uitgangspunt
7.2.3	Er behoort een formele en gecommuniceerde disciplinaire procedure te zijn om actie te ondernemen tegen medewerkers die een inbreuk hebben gepleegd op de informatiebeveiliging.	Bij geconstateerde inbreuk op het informatiebeveiligingsbeleid door een medewerker van Leverancier zal deze de toegang tot de omgeving van Opdrachtgever direct en permanent geweigerd worden. De medewerker mag geen werkzaamheden meer verrichten in het kader van deze Overeenkomst.
8.1.3.1	Alle medewerkers zijn aantoonbaar gewezen op de gedragsregels voor het gebruik van bedrijfsmiddelen.	Leverancier toont dit aan, de bedrijfsmiddelen van Opdrachtgever waaronder licenties, gegevens en configuraties worden enkel gebruikt voor het doel waarvoor ze beschikbaar worden gesteld.
8.1.3.2	De gedragsregels voor het gebruik van bedrijfsmiddelen zijn voor extern personeel in het contract vastgelegd overeenkomstig de huisregels of gedragsregels.	Leverancier toont dit aan.
8.1.4	Alle medewerkers en externe gebruikers moeten alle bedrijfsmiddelen van de organisatie die ze in hun bezit hebben bij beëindiging van hun dienstverband, contract of overeenkomst terug te geven.	Leverancier toont dit aan.
8.2.1.1	De informatie in alle informatiesystemen is door middel van een expliciete risicoafweging geclassificeerd, zodat duidelijk is welke bescherming nodig is.	Leverancier bevestigt de classificatie (BBN-2) die door Opdrachtgever aan datasets of andere gegevens is gegeven te respecteren en daarvoor passende controls conform dit document te hanteren.
8.2.2	Om informatie te labelen behoort een passende reeks procedures te worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.	Leverancier toont aan maatregelen te hebben getroffen om te voorkomen dat ongeautoriseerden kennis kunnen nemen van datasets of andere gegevens van Opdrachtgever.
8.3.1.1	Er is een verwijderinstructie waarin is opgenomen dat van verwijderbare media die herbruikbaar zijn en die de organisatie verlaten de onnodige inhoud onherstelbaar verwijderd is (ISO 27002 – implementatierichtlijn 8.3.1.a).	Leverancier toont dit aan.
8.3.2.1	Media die vertrouwelijke informatie bevatten, zijn opgeslagen op een plek die niet toegankelijk is voor onbevoegden.	Leverancier toont dit aan.
8.3.2.2	Verwijdering vindt plaats op een veilige manier, bijvoorbeeld door verbranding of versnippering. Verwijdering van alleen gegevens is ook mogelijk door het wissen van de gegevens voordat de media worden gebruikt voor een andere toepassing in de organisatie (ISO 27002 – implementatierichtlijn 8.3.2.a).	Zie 8.3.1.1.

BIO nr.	Control / Beveiligingsmaatregel	Eis / uitgangspunt
9.1.2.1	Alleen geauthenticeerde apparatuur kan toegang krijgen tot een vertrouwde zone.	Opdrachtgever hanteert een persoonlijke multi-factor authenticatie, met inachtneming van de vereisten aan een wachtwoord in hoofdstuk 13. Leverancier gaat hiermee akkoord.
9.1.2.2	Gebruikers met eigen of ongeauthenticeerde apparatuur (Bring Your Own Device) krijgen alleen toegang tot een onvertrouwde zone.	Om toegang te krijgen tot het VOR-IN netwerk dient een gebruiker altijd van het door de Leverancier beheerde netwerk gebruik maken.
9.2.1.1	Er is een sluitende formele registratie- en afmeldprocedure voor het beheren van gebruikersidentificaties.	Leverancier toont dit aan.
9.2.1.2	Het gebruiken van groepsaccounts is niet toegestaan tenzij dit wordt gemotiveerd en vastgelegd door de proceseigenaar.	Opdrachtgever staat het gebruik van groepsaccounts niet toe, Leverancier gaat hiermee akkoord.
9.2.2.1	Er is uitsluitend toegang verleend tot informatiesystemen na autorisatie door een bevoegde functionaris.	Autorisaties worden vastgelegd in een autorisatiematrix. Opdrachtgever verleent enkel toegang aan medewerkers in de autorisatiematrix die voldoen aan de gestelde eisen (onder andere hoofdstuk 7).
9.2.2.2	Op basis van een risicoafweging is bepaald waar en op welke wijze functiescheiding wordt toegepast en welke toegangsrechten worden gegeven.	Leverancier toont aan op welke wijze de risicoafweging plaatsvindt.
9.2.2.3	Er is een actueel mandaatregister of er zijn functieprofielen waaruit blijkt welke personen bevoegdheden hebben voor het verlenen van toegangsrechten.	Dit wordt opgenomen in de autorisatiematrix. Leverancier levert de autorisatiematrix aan voorafgaand aan de ingebruikname van de IDMA
9.2.3.1	De uitgegeven speciale bevoegdheden worden minimaal ieder kwartaal beoordeeld.	Leverancier toont dit aan. Het initiatief voor het doorgeven van wijzigingen ligt bij Leverancier.
9.2.5.2	De opvolging van bevindingen is gedocumenteerd en wordt behandeld als beveiligingsincident.	Leverancier gaat hiermee akkoord.
9.2.5.3	Alle uitgegeven toegangsrechten worden minimaal eenmaal per halfjaar beoordeeld.	Het initiatief voor het doorgeven van wijzigingen ligt bij Leverancier. De toegangsrechten (autorisatiematrix) wordt elk kwartaal beoordeeld.
9.2.6	De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatie verwerkende faciliteiten behoren bij beëindiging van hun dienstverband, contract of overeenkomst te worden verwijderd, en bij wijzigingen behoren ze te worden aangepast.	Leverancier toont dit aan middels autorisatieprocedure voor in-, uit- en doorstroom.

BIO nr.	Control / Beveiligingsmaatregel	Eis / uitgangspunt
9.3.1.1	Medewerkers worden ondersteund in het beheren van hun wachtwoorden door het beschikbaar stellen van een wachtwoordenkluis.	Leverancier geeft aan welke middelen hiertoe ter beschikking worden gesteld
9.4.1.2	Gebruikers kunnen alleen die informatie met specifiek belang inzien en verwerken die ze nodig hebben voor de uitoefening van hun taak.	In de autorisatiematrix is aangegeven welke informatie door wie wordt ingezien.
9.4.2.1	Als vanuit een onvertrouwde zone toegang wordt verleend naar een vertrouwde zone, gebeurt dit alleen op basis van minimaal two-factor authenticatie.	Zie 9.1.2.1.
9.4.2.2	Voor het verlenen van toegang tot het netwerk aan externe leveranciers wordt vooraf een risicoafweging gemaakt. De risicoafweging bepaalt onder welke voorwaarden de leveranciers toegang krijgen. Uit een registratie blijkt hoe de rechten zijn toegekend.	Voor externe leveranciers gelden dezelfde uitgangspunten als voor eigen medewerkers. Leverancier bevestigt dit.
9.4.3.1	Als er geen gebruik wordt gemaakt van two factor authenticatie is de wachtwoordlengte minimaal 8 posities en complex van samenstelling. Vanaf een wachtwoordlengte van 20 posities vervalt de complexiteitseis. Het aantal inlogpogingen is maximaal 10. De tijdsduur dat een account wordt geblokkeerd na overschrijding van het aantal keer foutief inloggen is vastgelegd.	Opdrachtgever staat niet toe dat er géén gebruik wordt gemaakt van two-factor authenticatie. De te gebruiken wachtwoorden dienen te voldoen aan deze richtlijn.
9.4.3.2	In situaties waar geen two-factor authenticatie mogelijk is, wordt minimaal halfjaarlijks het wachtwoord vernieuwd (zie ook 9.4.2.1.).	Opdrachtgever staat niet toe dat er geen gebruik wordt gemaakt van two-factor authenticatie. Wachtwoorden worden elke 3 maanden vernieuwd.
9.4.3.3	Het wachtwoordbeleid wordt geautomatiseerd afgedwongen.	Voor toegang tot de managementserver dwingt Opdrachtgever dit af.
9.4.3.4	Initiële wachtwoorden en wachtwoorden die gereset zijn, hebben een maximale geldigheidsduur van een werkdag en moeten bij het eerste gebruik worden gewijzigd.	Voor toegang tot de managementserver dwingt Opdrachtgever dit af.
9.4.3.5	Wachtwoorden die voldoen aan het wachtwoordbeleid hebben een maximale geldigheidsduur van een jaar. Daar waar het beleid niet toepasbaar is, geldt een maximale geldigheidsduur van 6 maanden.	Voor toegang tot de managementserver dwingt Opdrachtgever dit af (maximale geldigheidsduur van 3 maanden).
9.4.4.1	Alleen bevoegd personeel heeft toegang tot systeemhulpmiddelen.	Leverancier heeft dit vastgelegd in zijn informatiebeveiligingsbeleid.
9.4.4.2	Het gebruik van systeemhulpmiddelen wordt gelogd. De logging is een halfjaar beschikbaar voor onderzoek.	Leverancier heeft dit vastgelegd in zijn informatiebeveiligingsbeleid.

BIO nr.	Control / Beveiligingsmaatregel	Eis / uitgangspunt
10.1.1.1	In het cryptografiebeleid zijn minimaal de volgende onderwerpen uitgewerkt: a) wanneer cryptografie ingezet wordt; b) wie verantwoordelijk is voor de implementatie; c) wie verantwoordelijk is voor het sleutelbeheer; d) welke normen als basis dienen voor cryptografie en de wijze waarop de normen van het Forum worden toegepast; e) de wijze waarop het beschermingsniveau vastgesteld wordt; f) bij inter-organisatie communicatie wordt het beleid onderling vastgesteld.	Leverancier heeft dit vastgelegd in zijn cryptografiebeleid
10.1.1.2	Cryptografische toepassingen voldoen aan passende standaarden.	Opdrachtgever dwingt minimaal TLS 1.2 af op verbindingen.
10.1.2.1	Ingeval van PKI-overheid certificaten: hanteer de PKI-Overheid-eisen t.a.v. het sleutelbeheer. In overige situaties: hanteer de standaard ISO-11770 voor het beheer van cryptografische sleutels.	Indien PKI-overheid certificaten toegepast worden, zal Leverancier zich conformeren en meewerken aan de migratie.
10.1.2.2	Er zijn (contractuele) afspraken over reservecertificaten van een alternatieve leverancier als uit risicoafweging blijkt dat deze noodzakelijk zijn.	Indien van toepassing zal Leverancier zich conformeren en meewerken aan de migratie.
11.1.1.1	Er wordt voor het inrichten van beveiligde zones gebruik gemaakt van standaarden.	Leverancier verklaart welke standaarden hiervoor geïmplementeerd zijn.
11.1.2.1	In geval van concrete beveiligingsrisico's worden waarschuwingen, conform onderlinge afspraken, verzonden aan de relevante collega's binnen het beveiligingsdomein van de overheid.	Leverancier bevestigt bij beveiligingsincidenten en datalekken direct Opdrachtgever in te lichten.
11.1.5	Voor het werken in beveiligde gebieden behoren procedures te worden ontwikkeld en toegepast.	Zonder expliciete toestemming van Opdrachtgever mogen geen foto's, video-opnames, of geluidsopnames worden gemaakt in beveiligde ruimtes, waaronder de Verkeerscentrale.
11.2.9.1	Een onbemende werkplek is altijd vergrendeld.	Leverancier heeft dit vastgelegd in zijn informatiebeveiligingsbeleid.
11.2.9.2	Informatie wordt automatisch ontoegankelijk gemaakt met bijvoorbeeld een screensaver na een inactiviteit van maximaal 15 minuten.	Leverancier heeft dit vastgelegd in zijn informatiebeveiligingsbeleid.
11.2.9.3	Sessies op remote desktops worden op het remote platform vergrendeld na een vastgestelde periode.	Leverancier heeft dit vastgelegd in zijn informatiebeveiligingsbeleid.
11.2.9.4	Het overnemen van sessies op remote werkplekken op een andere werkplek is alleen mogelijk via dezelfde beveiligde loginprocedure als waarmee de sessie is gecreëerd. Na een expliciete risicoafweging mag hiervan worden afgeweken.	Leverancier heeft dit vastgelegd in zijn informatiebeveiligingsbeleid.

BIO nr.	Control / Beveiligingsmaatregel	Eis / uitgangspunt
11.2.9.5	Bij het gebruik van een chipcardtoken voor toegang tot systemen wordt bij het verwijderen van het token de toegangsbeveiligingslock automatisch geactiveerd.	Leverancier heeft dit vastgelegd in zijn informatiebeveiligingsbeleid.
12.1.1	Bedieningsprocedures behoren te worden gedocumenteerd en beschikbaar te worden gesteld aan alle gebruikers die ze nodig hebben	Leverancier levert hiertoe training en handleiding(en), conform het Programma van Eisen.
12.1.2.1	In de procedure voor wijzigingenbeheer is minimaal aandacht besteed aan: a) het administreren van wijzigingen; b) risicoafweging van mogelijke gevolgen van de wijzigingen; c) goedkeuringsprocedure voor wijzigingen.	Leverancier toont dit aan middels zijn gehanteerde proces voor wijzigingsbeheer. Dit wordt vastgelegd in de DAP.
12.1.4.1	In de productieomgeving wordt niet getest. Alleen met voorafgaande goedkeuring door de proceseigenaar en schriftelijke vastlegging hiervan, kan hierop worden afgeweken.	Leverancier toont aan te beschikken over geschikte testfaciliteiten. Opdrachtgever beschikt over een acceptatieomgeving.
12.1.4.2	Wijzigingen op de productieomgeving worden altijd getest voordat zij in productie gebracht worden. Alleen met voorafgaande goedkeuring door de proceseigenaar en schriftelijke vastlegging hiervan, kan hierop worden afgeweken.	Leverancier handelt hiernaar.
12.2.1.1	Het downloaden van bestanden is beheerst en beperkt op basis van risico en need-of-use.	Leverancier toont dit aan middels documentatie van zijn gehanteerde beheerproces.
12.2.1.2	Gebruikers zijn voorgelicht over de risico's ten aanzien van surfgedrag en het klikken op onbekende linken.	Leverancier toont aan dat dit onderdeel is van bewustwording maatregelen (zie hoofdstuk 7)
12.2.1.3	De gebruikte antimalwaresoftware en bijbehorende herstelsoftware is actueel en wordt ondersteund door periodieke updates.	Leverancier toont dit aan middels documentatie van zijn gehanteerde beheerproces.
12.2.1.4	Computers en media worden als voorzorgsmaatregel routinematig gescand. De uitgevoerde scan behoort te omvatten: a) alle bestanden die via netwerken of via elke vorm van opslagmedium zijn ontvangen, vóór gebruik op malware scannen; b) bijlagen en downloads vóór gebruik.	Leverancier toont dit aan middels documentatie van zijn gehanteerde beheerproces.
12.2.1.5	De malware scan wordt op verschillende omgevingen uitgevoerd, bijv. op mailservers, desktopcomputers en bij de toegang tot het netwerk van de organisatie.	Leverancier toont dit aan middels documentatie van zijn gehanteerde beheerproces.
12.3.1.1	Er is een back-up beleid waarin de eisen voor het bewaren en beschermen zijn gedefinieerd en vastgesteld.	Leverancier toont dit aan middels documentatie backup proces.

BIO nr.	Control / Beveiligingsmaatregel	Eis / uitgangspunt
12.3.1.5	De restore procedure wordt minimaal jaarlijks getest of na een grote wijziging om de goede werking te waarborgen als deze in noodgevallen uitgevoerd moet worden.	Leverancier toont dit aan, met betrekking tot de (ontwikkel en test) applicatie versies.
12.4.1.1	Een logregel bevat minimaal de gebeurtenis; de benodigde informatie die nodig is om het incident met hoge mate van zekerheid te herleiden tot een natuurlijk persoon; het gebruikte apparaat; het resultaat van de handeling; een datum en tijdstip van de gebeurtenis.	Leverancier toont dit aan middels lograpportage.
12.4.1.2	Een logregel bevat in geen geval gegevens die tot het doorbreken van de beveiliging kunnen leiden.	Leverancier toont dit aan middels lograpportage.
12.4.2.1	Er is een overzicht van logbestanden die worden gegenereerd.	Leverancier toont dit aan.
12.4.2.2	Ten behoeve van de loganalyse is op basis van een expliciete risicoafweging de bewaarperiode van de logging bepaald. Binnen deze periode is de beschikbaarheid van de loginformatie gewaarborgd.	Leverancier toont dit aan.
12.4.2.3	Er is een (onafhankelijke) interne audit procedure die minimaal half jaarlijks toetst op het ongewijzigd bestaan van logbestanden.	Leverancier toont dit aan.
12.4.2.4	Oneigenlijk wijzigen, verwijderen of pogingen daartoe van loggegevens worden zo snel mogelijk gemeld als beveiligingsincident via de procedure voor informatiebeveiligingsincidenten conform hoofdstuk 16.	Leverancier toont aan dat dit onderdeel is van procedure informatie/beveiligingsincidenten.
12.6.1.1	Als de kans op misbruik en de verwachte schade beide hoog zijn (NCSC classificatie kwetsbaarheidswaarschuwingen), worden patches zo snel mogelijk, maar uiterlijk binnen een week geïnstalleerd. In de tussentijd worden op basis van een expliciete risicoafweging mitigerende maatregelen getroffen.	Leverancier stemt hiermee in.
13.1.2.1	Het dataverkeer dat de organisatie binnenkomt of uitgaat wordt bewaakt / geanalyseerd op kwaadaardige elementen middels detectievoorzieningen (zoals beschreven in de richtlijn voor implementatie van detectieoplossingen), zoals het Nationaal Detectie Netwerk (alleen voor rijksoverheidsorganisaties) of GDI, die worden ingezet op basis van een risico-inschatting, mede aan de hand van de aard van de te beschermen gegevens en informatiesystemen.	Leverancier toont aan middels beschreven procedure dat wijzigingsbeheer conform deze maatregelen is vastgelegd.
13.1.2.3	Bij draadloze verbindingen zoals wifi en bij bedrade verbindingen buiten het gecontroleerd gebied wordt gebruik gemaakt van encryptiemiddelen waarvoor het NBV een positief inzetadvies heeft afgegeven.	Leverancier toont dit aan middels beleidsstukken waarin dit beschreven is.

BIO nr.	Control / Beveiligingsmaatregel	Eis / uitgangspunt
13.1.2.4	In koppelpunten met externe of onvertrouwde zones zijn maatregelen getroffen om mogelijke aanvallen die de beschikbaarheid van de informatievoorziening negatief beïnvloeden (bijvoorbeeld DDoS-aanvallen, Distributed Denial of Service attacks) te signaleren en hierop te reageren.	Leverancier toont dit aan middels beleidsstukken waarin dit beschreven is.
13.1.3.1	Alle gescheiden groepen hebben een gedefinieerd beveiligingsniveau.	Leverancier toont dit aan. Opdrachtgever past netwerksegmentering toe tussen systemen.
13.2.3.1	Voor de beveiliging van elektronische (e-mail)berichten gelden de vastgestelde open standaarden tegen phishing en af luisteren op de 'pas toe of leg uit'-lijst van het Forum. Voor beveiliging van websiteverkeer gelden de open standaarden tegen af luisteren op de 'pas toe of leg uit'-lijst van het Forum.	Leverancier toont dit aan. Een webinterface moet volgens het 'pas toe of leg' principe beschermd te zijn tegen misbruik conform relevante normen en standaarden, waaronder OWASP® Application Security Verification Standaard (OWASP ASVS).
14.1.1.1	Bij nieuwe informatiesystemen en bij wijzigingen op bestaande informatiesystemen moet een expliciete risicoafweging worden uitgevoerd ten behoeve van het vaststellen van de beveiligingseisen, uitgaande van de BIO.	Leverancier conformeert zich hieraan.
14.2.1.1	De gangbare principes rondom Security by design zijn uitgangspunt voor de ontwikkeling van software en systemen	Leverancier toont dit aan.
14.2.2.1	Wijzigingsbeheer vindt plaats op basis van een algemeen geaccepteerd beheerframework.	Leverancier toont dit aan.
14.2.6.1	Systeemontwikkelomgevingen worden passend beveiligd op basis van een expliciete risicoafweging.	Leverancier toont dit aan middels risicomanagementproces waaruit dit blijkt.
14.2.9.1	Voor acceptatietesten van systemen worden gestructureerde testmethodieken gebruikt. De testen worden bij voorkeur geautomatiseerd uitgevoerd.	Leverancier toont dit aan middels opgave van procedurebeschrijving acceptatietesten.
14.2.9.2	Van de resultaten van de testen wordt verslag gemaakt.	Leverancier toont dit aan middels voorbeeld. De verslagen dienen als vertrouwelijk document beschouwd te worden voor alle betrokken partijen.
15.1.3.1	Leveranciers moeten hun keten van toeleveranciers bekend maken en transparant zijn over de maatregelen die zij genomen hebben om de aan hun opgelegde eisen ook door te vertalen naar hun toeleveranciers.	Leverancier toont dit aan middels documenten en procedure beschrijvingen.
15.2.1.1	Jaarlijks wordt de prestatie van leveranciers op het gebied van informatiebeveiliging beoordeeld op vooraf vastgestelde prestatie-indicatoren, zoals in het contract opgenomen is.	Conform Programma van Eisen en SLA.

BIO nr.	Control / Beveiligingsmaatregel	Eis / uitgangspunt
16.1.2.1	Er is een meldloket waar beveiligingsincidenten kunnen worden gemeld.	Leverancier toont aan te beschikken over een meldloket.
16.1.2.2	Er is een meldprocedure waarin de taken en verantwoordelijkheden van het meldloket staan beschreven.	Leverancier toont dit aan met documentatie.
16.1.2.3	Alle medewerkers en contractanten hebben aantoonbaar kennis genomen van de meldingsprocedure van incidenten.	Leverancier toont dit aan.
16.1.2.4	Incidenten worden zo snel mogelijk, maar in ieder geval binnen 24 uur na bekendwording, intern gemeld.	Leverancier toont dit aan middels incidentmanagementproces.
16.1.2.5	De proceseigenaar is verantwoordelijk voor het oplossen van beveiligingsincidenten.	Leverancier toont aan dat proces is ingericht en stemt in met oplossing van beveiligingsincidenten.
16.1.2.6	De opvolging van incidenten wordt maandelijks gerapporteerd aan de verantwoordelijke.	Leverancier toont aan dit te hebben vastgelegd en levert voorbeeldrapportage aan.
16.1.2.7	Informatie afkomstig uit de Coordinated Vulnerability Disclosure (CVD) procedure is onderdeel van de incidentrapportage.	Publieke bekendmaking van beveiligingsincidenten wanneer deze ook andere wegbeheerders of belanghebbenden raken zal volgens het principe van Responsible Disclosure procedure plaatsvinden. Deze melding wordt gedaan bij de Informatie Beveiligingsdienst (IBD) van de VNG.
16.1.4.1	Informatiebeveiligingsincidenten die hebben geleid tot een vermoedelijk of mogelijk opzettelijke inbreuk op de beschikbaarheid, vertrouwelijkheid of integriteit van informatie verwerkende systemen, behoren zo snel mogelijk (binnen 72 uur) al dan niet geautomatiseerd te worden gemeld aan het NCSC (alleen voor rijksoverheidsorganisaties) of de sectorale CERT.	Leverancier meldt binnen 48 uur aan Opdrachtgever, conform SLA.
16.1.6.1	Beveiligingsincidenten worden geanalyseerd met als doel te leren en het voorkomen van toekomstige beveiligingsincidenten.	De opdrachtnemer is verplicht beveiligingsincidenten te analyseren middel een Root Cause Analysis (RCA), met als doel te leren en te voorkomen van toekomstige beveiligingsincidenten. Na analyse dienen de mitigerende maatregelen bekend gemaakt te worden aan de opdrachtgever.
16.1.7.1	In geval van een (vermoed) informatiebeveiligingsincident is de bewaartermijn van de gelogde incidentinformatie minimaal drie jaar.	Leverancier toont dit aan.
17.1.3.1	Continuïteitsplannen worden jaarlijks getest op geldigheid en bruikbaarheid.	Leverancier toont dit aan.

BIO nr.	Control / Beveiligingsmaatregel	Eis / uitgangspunt
18.1.3.1	De proceseigenaar heeft per soort informatie inzichtelijk gemaakt wat de bewaartermijn is.	Verwerkt in eisen in PVE. Leverancier stelt bewaartermijnen overzicht op en beschikbaar.
18.1.4.1	In overeenstemming met de AVG heeft iedere organisatie een Functionaris Gegevensbescherming (FG) met voldoende mandaat om zijn/haar functie uit te voeren.	Leverancier toont dit aan.
18.1.4.2	Organisaties controleren regelmatig de naleving van de privacy regels en informatieverwerking en –procedures binnen haar verantwoordelijkheidsgebied aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging.	Leverancier toont opzet, bestaan en werking hiervan aan.
18.1.5.1	Cryptografische beheersmaatregelen moeten expliciet aansluiten bij de standaarden op de 'pas toe of leg uit'-lijst van het Forum.	Leverancier toont dit aan.
18.2.1.1	Er is een information security information system (ISMS) waarmee aantoonbaar de gehele plan-do-check-act cyclus op gestructureerde wijze wordt afgedekt.	Leverancier toont dit aan.
18.2.1.2	Er is een vastgesteld auditplan waarin jaarlijks keuzes worden gemaakt voor welke systemen welk soort beveiligingsaudits worden uitgevoerd.	Leverancier toont dit aan.
18.2.2.1	In de P&C cyclus wordt gerapporteerd over informatiebeveiliging, resulterend in een jaarlijks af te geven In Control Verklaring (ICV) over de informatiebeveiliging. Indien voldoende herkenbaar kan de ICV voor informatiebeveiliging onderdeel zijn van de reguliere, Generieke verantwoording.	Leverancier toont dit aan.
18.2.3.1	Informatiesystemen worden jaarlijks gecontroleerd op technische naleving van beveiligingsnormen en risico's ten aanzien van de feitelijke veiligheid. Dit kan bijvoorbeeld door (geautomatiseerde) kwetsbaarheidsanalyses of penetratietesten.	Leverancier toont dit aan.