

ICT Eisen	Programma van ICT Eisen voor de levering van Plansoftware en software Toepasbare Regels
ICTe1	GIBIT-Inkoopvoorwaarden
	1 Opdrachtnemer gaat akkoord met de GIBIT-inkoopvoorwaarden van de gemeente Purmerend. De Gibit is leidend i.g.v. tegenstrijdigheden;
ICTe2	SaaS oplossing Plansoftware / Toepasbare Regels
	1 Voor 27 oktober 2021 heeft de opdrachtnemer een door de opdrachtgever geteste en geaccepteerde oplossing opgeleverd op basis van een volledige SaaS oplossing welke voldoet aan het programma van eisen en de afgesproken uitvoering van aangeboden wensen binnen de gunningscriteria;
	2 De opdrachtnemer levert een Plansoftware applicatie en/of een applicatie voor toepasbare regels op basis van een SaaS -oplossing;
	2.1 De oplossing wordt geleverd als een volledig gehoste SaaS oplossing.
	3 De opdrachtnemer garandeert dat gedurende de contractperiode de aangeboden oplossing wordt onderhouden, ondersteund en doorontwikkeld;
	4 Hosting betreft een voldoende beveiligde fysieke en logische omgeving – bestaande uit alle benodigde software (zoals virtualisatiesoftware, firewalls, technisch beheertools en back-upsoftware) en hardware (zoals serverapparatuur, opslag, back-upapparatuur en netwerken) – beschikbaar stellen van Plansoftware applicatie en/of een applicatie voor toepasbare regels, inclusief het uitvoeren van het (technisch) beheer van deze omgeving;
	5 Inkoop-eisen voor SaaS m.b.t. IP. Alle SaaS oplossingen moeten IPv4 en IPv6 ondersteunen en in staat zijn om te kunnen communiceren via IPv4-only, via IPv6-only en via dual-stack netwerken. Als de software netwerkparameters in haar lokale of remote server-instellingen bevat, dan moet de software ook de configuratie van IPv6-parameters ondersteunen. Alle functies die via IPv4 worden aangeboden moeten ook via IPv6 beschikbaar zijn. De opdrachtgever/eindgebruiker mag geen verschil ervaren wanneer de software via IPv4 of IPv6 communiceert, tenzij dit een expliciet voordeel voor de gebruiker oplevert. Het wordt ten eerste afgeraden om vaste IPv6 adressen in de softwarecode op te nemen.
	6 De Plansoftware applicatie en/of de applicatie voor toepasbare regels is een webbased oplossing en het front-end voor de medewerkers van de opdrachtgever bestaat uit een webapplicatie;
	7 De Plansoftware applicatie en/of de applicatie voor toepasbare regels is volledig in het Nederlands in woord en geschrift;
ICTe3	Doelgroep gebruikers
	1 De door de opdrachtnemer geleverde SaaS -oplossing geeft het recht tot gebruik van de Plansoftware applicatie en/of de applicatie voor toepasbare regels door alle medewerkers van de opdrachtgever en uitvoeringsorganisaties voor zover deze taken uitvoeren voor de opdrachtgever.
ICTe4	Beschikbaarheid
	1 De SaaS-oplossing is 99,5% beschikbaar;
	3 Onderhoudstijden van opdrachtnemer vinden plaats na werktijden (ICTe4.1) in de avonden, weekenden en op nationale feestdagen;
	4 Opdrachtnemer hanteert een vast jaarlijks upgrade schema;
	5 Werkzaamheden door de opdrachtnemer worden altijd minimaal 14 werkdagen van tevoren gecommuniceerd;
	6 Een uitzondering op punten ICTe4.2, ICTe4.3, ICTe4.4 en ICTe4.5 zijn calamiteiten met een hoge prioriteit zoals onvoorziene zaken waarbij de integriteit van de gegevens in gevaar zijn, informatieveiligheidsincidenten en rampen;
ICTe5	Performance
	1 De opdrachtnemer draagt zorg voor een SaaS-oplossing met voldoende (in praktijk gangbare en acceptabele) prestaties voor de eindgebruiker, hierbij moet worden uitgegaan van circa 20 concurrent eindgebruikers per applicatie;
	2 De opdrachtnemer voorkomt dat gebruik van gedeelde componenten door andere klanten in de infrastructuur de performance bedreigen;
ICTe6	Wijzigingenbeheer geïnitieerd door opdrachtnemer
	1 Wijzigingen door de opdrachtnemer doorgevoerd in de SaaS -oplossing welke van invloed kunnen zijn op de data integriteit, informatieveiligheid, privacywetgeving, beschikbaarheid, toegankelijkheid, functionele werking, koppelvlakken, etc. worden vooraf afgestemd in het gebruikersoverleg. Wijzigingsprocedure met minimaal de aandacht voor: - het administreren van significante wijzigingen (Release note); - impactanalyse van mogelijke gevolgen van de wijzigingen (Release note); - goedkeuringsprocedure voor wijzigingen.
	2 Alle wijzigingen worden door de opdrachtnemer altijd eerst getest voordat deze in productie worden genomen en worden via wijzigingsprocedure doorgevoerd;
	3 Relevante wijzigingen van de opdrachtnemer binnen de SaaS -oplossing worden gelogd en zijn opvraagbaar door de opdrachtgever;
ICTe7	Technische beveiliging
	1 De opdrachtnemer zorgt voor een gedegen domeinscheiding tussen de SaaS -oplossing van de opdrachtgever en andere domeinen;
	2 De opdrachtnemer is verantwoordelijk voor een jaarlijkse uitwijktest en de rapportage over de test wordt gedeeld met de opdrachtgever;

	3 De opdrachtnemer hanteert een degelijk patchschema om alle componenten (zoals firmware, operating systems, applicaties) van de gehoste SaaS-oplossing actueel te houden om verbeteringen door te voeren en bekende fouten op te lossen;
	4 De opdrachtnemer geeft hoge prioriteit aan het snel installeren van de laatste beveiligingspatches;
	5 De opdrachtnemer maakt gebruik van een hardeningsproces zodat alle ICT-componenten zijn gehard tegen aanvallen (het realiseren van deze acties leidt tot een beter beveiligd systeem dat moeilijker door kwaadwillende is te misbruiken).
	6 Toegang tot de SaaS-oplossing voor medewerkers van de opdrachtgever is alleen mogelijk vanuit afgesproken vaste IP-adressen van de opdrachtgever en over een veilige verbinding;
	7 Er wordt geen gebruik gemaakt van onbeveiligde of publieke internetverbindingen. Uitzondering hierop kan zijn een met de opdrachtgever afgesproken beveiligde uitwijkverbinding over het publieke internet om calamiteiten op te vangen;
	8 De opdrachtnemer zorgt ervoor dat opdrachtgever geen last heeft van onwenselijk gedrag van andere klanten (bijv. spamming vanuit eenzelfde IP-adres);
	9 Bij het sturen en ontvangen van e-mails wordt gebruik gemaakt van alle hiervoor relevante, voor overheden verplichte, beveiligingsstandaarden. Oplossing voldoet aan de vereiste van het forum voor standaardisatie gedurende de looptijd van het contract.
	10 De opdrachtnemer zorgt ervoor dat netwerkverkeer tussen verschillende omgevingen niet kan worden onderschept door andere klanten die actief zijn binnen de systeemomgeving van opdrachtnemer;
	11 De opdrachtnemer voert actief controles uit op systeemlogging;
	12 Situaties waarin meer dan normale kwetsbaarheden of risico's aanwezig zijn, worden onmiddellijk gemeld aan en besproken met de opdrachtgever;
	13 IT-voorzieningen en apparatuur bij opdrachtnemer zijn fysiek beschermd tegen toegang door onbevoegden en tegen schade en storingen;
ICTe8	Technisch beheer
	1 Systeem en Technisch beheer wordt geheel verzorgd door opdrachtnemer;
	2 Technisch Applicatiebeheer betreft de werkzaamheden die nodig zijn voor het waarborgen van de ononderbroken goede werking van de SaaS-oplossing van de Plansoftware applicatie en/of de applicatie voor toepasbare regels ;
	3 Technisch Applicatiebeheer omvat het installeren en (v.w.b. technische aspecten) testen van nieuwe en verbeterde versies van de Plansoftware applicatie en/of de applicatie voor toepasbare regels, die beschikbaar komen naar aanleiding van onderhoud, in de gehele OTAP-straat;
	4 Technisch Applicatiebeheer omvat tevens het continu en actief monitoren van o.a. de beschikbaarheid, capaciteit, continuïteit, back-up, beveiliging en data-integriteit van de Plansoftware applicatie en/of de applicatie voor toepasbare regels;
	5 Rollen en rechten van zowel de opdrachtnemer (technisch beheer) als de opdrachtgever (functioneel beheerders) zijn inzichtelijk. Gebruikers van opdrachtgever worden enkel aangemaakt door opdrachtnemer na opdracht van een bevoegd ambtenaar van de opdrachtgever.
ICTe9	Functioneel beheer
	1 Voor het functioneel beheer van het systeem is geen programmeerkennis nodig (principe van klikken en niet tikken);
	2 Het systeem voorziet in een scheiding tussen systeembeheer, technisch- en functioneel beheer;
	3 Voor het uitvoeren van functioneel beheer moet de functioneel beheerder zelf de autorisaties (rollen en rechten) en stamtabellen kunnen inrichten en beheren met begin- en einddatum en gebruikmakend van logfiles. Voorbeelden daarvan zijn het aanmaken en wijzigen van gebruikers, functierollen, stuur- en stamgegevens ;
ICTe10	OTAP-architectuur
	1 De door de opdrachtnemer geleverde Plansoftware applicatie en/of de applicatie voor toepasbare regels dient te worden uitgevoerd in een OTAP-architectuur (ontwikkel, test, acceptatie, productie). Er worden minimaal 2 separate omgevingen geleverd (te weten P en OTA). Alle benodigde licenties om dit te realiseren dienen aangeboden te worden;
	2 De OTA omgeving is voor de beheerder als de gebruiker vrij te gebruiken
	3 De OTA omgeving is inzetbaar met behulp van geanonimiseerde gegevens.
	4 Na de ingebruikname van de Productieomgeving zal de OTA-omgeving beschikbaar moeten blijven als Testomgeving. De licentieverlening dient daarop zonder extra kosten voor de gemeente gebaseerd te zijn.
ICTe11	Toegang tot de Plansoftware applicatie en/of de applicatie voor toepasbare regels via webapplicatie
	1 De webapplicatie is bruikbaar op apparaten met het Windows 10 en hoger operating system, ook als het Windows operating systeem is gevirtualiseerd (SBC of VDI). Indien ook beschikbaar op iOS (iPad en iPhone) past de weergave van de webapplicatie zich aan het soort apparaat aan;
	2 De webapplicatie is toegankelijk en compatible met de meest recente Microsoft EDGE browser op basis van Chromium of Mozilla Firefox webbrowser, ; Indien webbased applicaties worden ingezet voor extern gebruik dan moeten zij kunnen functioneren op basis: a. Mozilla Firefox b. Google Chrome c. Microsoft Edge

3	Waar aanvullende softwarecomponenten aan kant van de client (gebruiker) noodzakelijk zijn kunnen deze componenten ook gevirtualiseerd worden met Microsoft APP-V vanaf versie 5.x; (Met softwarecomponenten wordt geduid op componenten welke een interactie hebben met de Webbrowser, een interactie hebben met bijvoorbeeld de lokale MS Office omgeving, DMS achtige functionaliteit of specifieke interface software zoals voor functioneel beheer.)
4	Voor een webbased applicatie gelden de onderstaande eisen. a. volledig HTML5 ondersteuning. b. het gebruik van JAVA is niet toegestaan zonder toestemming vooraf van de opdrachtgever.
4.1	Het gebruik van plug-ins is in afwijking op deze eis niet toegestaan zonder goedkeuring vooraf van de bevoegde ICT manager van de opdrachtgever.
4.1.1	Het gebruik van OpenGL of DirectX is niet toegestaan.
4.1.2	De toegang tot de webapplicatie maakt gebruik van een versleutelde (HTTPS) verbinding;
4.2	De webapplicatie controleert voor elk http-verzoek of de initiator geauthenticeerd is en de juiste autorisaties heeft;
4.3	De webapplicatie voldoet aan de beveiligingseisen die de NCSC/GOVCERT stelt aan de 5 kernpunten voor de beveiliging van webapplicaties: patching, invoervalidatie, uitvoervalidatie, sessieonderhoud, en databasegebruik. Zie hiervoor https://docplayer.nl/10466800-Checklist-beveiliging-webapplicaties.html
4.4	De webapplicatie slaat gevoelige gegevens versleuteld of gehashed op;
ICTe12	Informatieveiligheid
1	De opdrachtnemer houdt zich aan de naleving van alle wet- en regelgeving (Nederlandse en Europese) aangaande privacybescherming m.b.t. de door hem geleverde oplossing en diensten. Alle wet en regelgeving zoals de GDPR/AVG zijn leidend i.g.v. tegenstrijdigheden met andere eisen, wensen of voorstellen van opdrachtgever en opdrachtnemer;
2	De gegevens van opdrachtgever worden alleen in EER opgeslagen;
3	De infrastructuur en organisatie van de inschrijver zijn adequaat beveiligd volgens ISO/IEC 27001:2017 of vergelijkbaar. Inschrijver levert ten tijde van het tekenen van de overeenkomst het certificaat met bijbehorende verklaring van toepasselijkheid aan opdrachtgever. Daarnaast is inschrijver bereid jaarlijks een verklaring van toepasselijkheid of getrouwheid (of vergelijkbaar) te verkrijgen via een onafhankelijke derde partij (TPM)
4	Vulnerability assessments (security scans) worden periodiek uitgevoerd (minimaal 1 x per jaar);
4.1	De opdrachtgever heeft toestemming om zelf een pentest te (laten) uitvoeren.
5	Rapportages omtrent de veiligheid van de Saas-oplossing worden gedeeld met de opdrachtgever;
6	De aangeboden oplossing legt een audit-trail vast over het gebruik van de Plansoftware applicatie en/of de applicatie voor toepasbare regels
6.1	Deze audit trail bevat alle handelingen m.b.t. gebruikersautorisaties en functioneel gebruik (van medewerkers opdrachtgever) van gevraagd systeem zoals raadplegen, aanmaken, muteren, verwijderen van informatie.
6.2	Vastlegging vindt minimaal plaats op gebruikersniveau en -rol, tijdstip en verrichte actie en is inzichtelijk voor zowel de functioneel beheerders als de CISO van de opdrachtgever;
6.3	Het systeem ondersteunt dat de logbestanden ten behoeve van de audittrail gedurende een door de opdrachtgever nader te bepalen periode bewaard worden waarna het mogelijk is deze uit het systeem te verwijderen.
7	De opdrachtnemer garandeert dat ongeautoriseerde personen geen toegang hebben tot gegevens of gegevensdragers (zoals harde schijven en back-upmedia) die tussentijds of na beëindiging van de overeenkomst worden verwijderd c.q. worden vervangen;
8	De opdrachtnemer zal indien hij (pogingen tot) ongeautoriseerde toegang tot de systeemomgeving signaleert, alle noodzakelijke maatregelen nemen teneinde de eventuele schade tot een minimum te beperken en herhaling te voorkomen. De (poging tot) ongeautoriseerde toegang alsmede alle getroffen maatregelen zullen direct aan de opdrachtgever worden gerapporteerd;
9	De opdrachtnemer verleent medewerking aan het uitoefenen van controle door of namens opdrachtgever op bewaring en gebruik van data en naleving van procedures;
10	De opdrachtnemer draagt zorg voor een toereikend back-up en restore proces van de Plansoftware applicatie en/of de applicatie voor toepasbare regels welke indien van toepassing ook voldoet aan de eisen inzake wettelijke bewaartermijnen;
11	In geval van toegang tot de Plansoftware applicatie en/of de applicatie voor toepasbare regels vanuit het netwerk van opdrachtgever wordt gebruik gemaakt van SSO. In geval van toegang tot de Plansoftware applicatie en/of de applicatie voor toepasbare regels van buiten het netwerk van opdrachtgever wordt gebruik gemaakt van Multi factor authenticatie.
12	Als op de Plansoftware applicatie en/of de applicatie voor toepasbare regels enkel vanaf het lokale netwerk ingelogd kan worden, dan dwingt het systeem een wachtwoord af van ten minste acht vrij te kiezen karakters waaronder het gebruik van een hoofdletter, cijfer en leesteken.
12.1	Als op de Plansoftware applicatie en/of de applicatie voor toepasbare regels vanaf het internet ingelogd kan worden, dan dient deze log-in methode op basis van twee factor authenticatie te gebeuren.
12.2	Het systeem ondersteunt het afdwingen van een maximale gebruiksduur van een wachtwoord. Indien opdrachtnemer hier niet aan kan voldoen kan van deze eis, na goedkeuring van bevoegd ICT manager van opdrachtgever, worden afgeweken.
12.3	De applicatie moet een functie hebben waarmee time-outs op het aantal foutieve inlogpogingen worden ondersteund. Onderscheid moet gemaakt kunnen worden tussen het inloggen vanaf het lokale netwerk of vanaf het internet. Indien opdrachtnemer hier niet aan kan voldoen kan van deze eis, na goedkeuring van bevoegd ICT manager van opdrachtgever, worden afgeweken.

12.4	De applicatie moet gebruikers en beheerders de mogelijkheid geven om hun wachtwoord te kunnen wijzigen. Beheerders van de opdrachtgever moeten de wachtwoorden van gebruikers kunnen wijzigen.
12.5	Het gebruik van de wachtwoorden van de Plansoftware applicatie en/of de applicatie voor toepasbare regels in de organisatie moet door beheerdersaccounts gecontroleerd/beheerd kunnen worden.
12.6	Indien de Plansoftware applicatie en/of de applicatie voor toepasbare regels van buiten ons netwerk benaderbaar is, dan moet de applicatie zichzelf na een door opdrachtgever in te stellen termijn aan in-activiteit vergrendelen.
12.7	Wachtwoorden in de Plansoftware applicatie en/of de applicatie voor toepasbare regels worden nooit in plaintext opgeslagen of verstuurd.
12.8	De Plansoftware applicatie en/of de applicatie voor toepasbare regels forceert een verandering van wachtwoord bij het eerste gebruik (ingebruikname) van het systeem door individuele gebruikers. Indien opdrachtnemer hier niet aan kan voldoen kan van deze eis, na goedkeuring van bevoegd ICT manager van opdrachtgever, worden afgeweken.
13	Het systeem voldoet aan de actuele vereisten gesteld in de NCSC beveiligingsrichtlijnen voor webapplicaties.
14	Voor veilige bestandsuitwisseling tussen opdrachtgever en opdrachtnemer accepteert opdrachtnemer de oplossing die opdrachtgever biedt (op dit moment ZIVVER). Indien leverancier een oplossing ter beschikking heeft kan dit na goedkeuring van bevoegd ICT manager van de opdrachtgever als alternatief dienen.
ICTe13	Koppelvlakken.
1	Er is een actief LDAP (AD-FS) koppelvlak met de AD van de opdrachtgever voor gebruikersbeheer (gebruiker, inlognaam en wachtwoord, account active/ disabled);
1.1	Opdrachtnemer ondersteunt het gebruik van AD Authenticatie ADFS staat voor Active Directory Federation-services, is een oplossing van Microsoft voor Single sign-on en web-gebaseerde authenticatie voor systemen en applicaties. De opdrachtgever maakt gebruik van Microsoft ADFS i.c.m. met Azure Multi-Factor Authentication. Protocollen die hierbij worden ondersteund zijn: •OpenID Connect (voorkeur) •OAuth (voorkeur) •WS-Federation, •WS-Trust, •SAML
2	De opdrachtnemer organiseert de afstemming en realisatie van de koppelingen (gegevensuitwisseling) met andere noodzakelijke applicaties van de opdrachtgever. De opdrachtgever heeft een ondersteunende rol;
2.1	De oplossing ondersteunt de onderstaande koppelvlakken met andere applicaties van de opdrachtgever: ADFS en DSO/Koop zoals aangegeven in de aanbestedingsleidraad en functionele eisen.
3	De applicatie ondersteunt waar relevant Microsoft Office; bijvoorbeeld rapportages naar Word. De extensie .doc wordt niet geaccepteerd. De email functie van Outlook 365 (Exchange Online) wordt ondersteund met gebruikmaking van de Microsoft Graph API. (EWS als protocol kan nu nog tijdelijk in afwijking op de eis van Graph worden ondersteund maar alleen toegestaan na een akkoord vooraf van de bevoegd manager ICT.) De opdrachtgever maakt gebruik van MS Office, de Plansoftware applicatie en/of de applicatie voor toepasbare regels moet hiermee compatible zijn.
5	Voor gebruik van Azure SQL gelden de volgende voorwaarden: De database wordt beveiligd door een firewall(rules) zodanig dat deze alleen door de applicatie kan worden benaderd, volgens de actuele best practices van Microsoft. •IP-filtering •Authenticatie •Beperkte toegang tot dataset
5.1	Voor oplossingen die van buiten benaderbaar zijn gelden TEVENs de eisen genoemd in de ICT Beveiligingsrichtlijnen voor webapplicaties van het NCSC. In het bijzonder hoofdstuk Uitvoeringsdomein>>Webapplicaties.
ICTe14	Uitwisselformaten
2	Uitwisselingen in- en export van gegevens vindt alleen plaats op een beveiligde wijze. Zonder de noodzaak van een directe user mapping naar een filesystem binnen de netwerkomgeving van de opdrachtgever of op de apparatuur van de gebruiker.
3	Indien binnen de looptijd van het contract een nieuwe StuF wordt uitgebracht dient u deze binnen 1 jaar na vaststelling van de nieuwe StuF-versie te ondersteunen;
ICTe15	Architectuur
1	Opdrachtnemer levert technische architectuurplaten van de Saas - oplossing en houdt deze gedurende de overeenkomst actueel;
2	De opdrachtnemer levert een technische architectuurplaat op hoofdlijnen met alle componenten, koppelvlakken, disaster/recovery en uitwijk (geografisch gescheiden datacenters);
3	De opdrachtnemer levert voor de oplevering minimaal de volgende documentatie: a. de architectuur van de applicatie b. datamodelspecificatie van de koppelvlakken
4	Opdrachtnemer zorgt ervoor dat benoemde documentatie actueel blijft.

	5 De opdrachtnemer draagt zorg voor een installatieverslag na elke installatie. Daarin is in elk geval opgenomen: een netwerktekening met gebruikte protocollen en poorten.
ICTe16	Support SLA
	1 Medewerkers van opdrachtnemer bieden ondersteuning in de Nederlandse taal in woord en geschrift;
	2 Opdrachtnemer levert voor de oplevering in de productieomgeving een Nederlandstalige handleiding voor de medewerkers van de opdrachtgever op;
	3 Opdrachtnemer beschikt over een helpdesk welke medewerkers van de opdrachtgever van maandag tot en met vrijdag van 8:00 tot 17:00 per telefoon te woord kan staan;
	4 Opdrachtnemer conformeert zich aan de gestelde eisen tot het handelen bij verstoringen conform onderstaande 'Vereisten bij verstoringen' ;
	5 Opdrachtnemer is verantwoordelijk voor het aanleveren en actueel houden van een contactenmatrix op functieniveau van alle betrokken medewerkers van zowel de opdrachtnemer als de opdrachtgever.
ICTe17	Opleiding
	1 De opdrachtnemer biedt inhouse (op locatie gemeente Purmerend) gebruikerstrainingen voor zowel functioneel beheerders als eindgebruikers, tenzij dit door geldende corona-maatregelen niet mogelijk is.
	2 Trainingen worden in het Nederlands gegeven; documentatie is in het Nederlands beschikbaar;
ICTe18	Overdracht gegevens/data bij beëindiging overeenkomst
	1 Alle gegevens in de Plansoftware applicatie en/of de applicatie voor toepasbare regels zijn en blijven te allen tijde eigendom van opdrachtgever en mogen door opdrachtnemer niet voor andere doeleinden worden gebruikt. Bij beëindiging van de overeenkomst worden alle gegevens overgedragen aan de opdrachtgever in een standaard uitwisselformaat.

Vereisten bij verstoringen		
De helpdesk is verantwoordelijk voor de gehele behandeling van meldingen, incidenten m.b.t. de Oplossing volgens de procedure zoals vastgelegd in de Service Level Agreement (SLA). De opdrachtgever bepaalt de prioriteit van incidenten. Ten aanzien van de ondersteuning wordt de volgende prioriteitsbepaling gehanteerd:		
Categorie	Type (ver)storing	Omschrijving
1	Kritisch	Applicatie is volledig niet beschikbaar
2	Groot	Applicatie is deels niet beschikbaar of deels niet beschikbaar voor 10% van de gebruikers
3	Klein	Kleine verstoringen
4	Vraag	Gebruikers of beheerdersvragen
De helpdesk draagt tevens zorg voor relateren van incidenten aan reeds bekende problemen m.b.t. de Oplossing. De Opdrachtnemer maakt voor de gemeente inzichtelijk wanneer een incident in behandeling is genomen en wat de status van afhandeling is. De Opdrachtnemer is eindverantwoordelijk voor het beheren van incidenten.		
Categorie	Reactietijd	Oplostijd
1	0 – ½ uur (op werkdagen tussen 08:00 en 17:00 uur)	Work-around binnen 4 uur, Oplossing binnen 8 uur
2	1 uur (op werkdagen tussen 08:00 en 17:00 uur)	Work-around binnen 8 uur op werkdagen, Oplossing binnen 24 uur op werkdagen
3	24 uur (op werkdagen tussen 08:00 en 17:00 uur)	Work-around binnen 2 werkdagen, Oplossing in volgende reguliere versie werkdagen
4	24 uur (op werkdagen tussen 08:00 en 17:00 uur)	Antwoord binnen 1 week
De opdrachtnemer meldt beveiligingsincident zo snel als mogelijk doch uiterlijk binnen 24 uur aan de opdrachtgever. Waarbij een incident wordt geclassificeerd en de volgende termijnen voor herstel worden gerealiseerd.		
Classificatie	Omschrijving	Hersteltijd
Extreem	Extreem hoog risico op gecompromitteerde beveiligingsinrichting met mogelijke catastrofale gevolgen op het gebied van financiën, reputatie etc.	4 uur
Hoog	Hoog risico op gecompromitteerde beveiligingsinrichting met mogelijke (significante) financieel, reputatie etc. gevolgen.	1 werkdag
Midden	Middelmatig risico op gecompromitteerde beveiligingsinrichting met minimale financieel, reputatie etc. gevolgen.	1 week
Laag	Laag risico op gecompromitteerde beveiligingscontrole met meetbare negatieve impact als resultaat.	2 weken