

Veiligheidsregio Noord-Holland Noord

Model Agenda leveranciersgesprekken

Documentinformatie

Naam document	Agenda leveranciersgesprekken
Classificatie	Intern
Eigenaar	Bianca Beerse
Versienummer	2019
Datum wijziging	28 juni 2019

Versiebeheer

Versie	Datum	Status	Door	Opmerkingen
2019	28 juni 2019	definitief	Bianca Beerse	

Inhoudsopgave

1. Begrippenlijst.....	2
2. Over dit document	2
3. Classificatie Overeenkomst.....	2
4. Periodieke afstemming.....	2
5. Agenda leveranciersgesprekken: ICT	3
6. Agenda leveranciersgesprekken: levering en dienstverlening.....	6

1. Begrippenlijst

Leverancier	Betrokken onderneming met welke de Overeenkomst is ondertekend. Voor deze specifieke Model agenda is dat << naam leverancier >>
Model agenda leveranciersgesprekken	Onderhavig document
Overeenkomst	Afgesloten (dienstverlenings-) overeenkomst waarop dit document betrekking heeft. Voor leesbaarheid van het stuk wordt de term Overeenkomst gebruikt.
Partijen	Alle betrokken ondernemingen welke de Overeenkomst hebben ondertekend. Voor deze specifieke Model agenda zijn partijen: - Veiligheidsregio Noord-Holland Noord - << naam leverancier >>
SLA	Service Level Agreement, wijze waarop invulling wordt gegeven aan de service afspraken betreffende Overeenkomst
VRNHN	Veiligheidsregio Noord-Holland Noord

2. Over dit document

Dit document bevat onderwerpen die VRNHN kan agenderen in periodieke gesprekken met leveranciers. Deze Model agenda is een integraal onderdeel van de aanbestedingsstukken, en wordt gelijktijdig gepubliceerd. Na ondertekening van de Overeenkomst wordt definitieve invulling gegeven aan de agendapunten. Per Overeenkomst dient de Model agenda ingevuld en aangepast te worden, passend bij de Overeenkomst.

3. Classificatie Overeenkomst

De Overeenkomst << naam overeenkomst >> is door VRNHN vanuit contractmanagement geclassificeerd als *hoog*. Bij deze Overeenkomst zijn de volgende risico's geïdentificeerd:

-
- ...

4. Periodieke afstemming

Vanuit de classificatie en risico's is het wenselijk periodieke afstemming te hebben om de prestaties van de leverancier te toetsen aan de Overeenkomst, waaronder de SLA en de overeengekomen prestaties vanuit het programma van Eisen, beantwoording van Wensen of andere afspraken.

Daarnaast is het van belang om de met Leverancier afgesproken procedures (DAP¹) periodiek te reviewen en actueel te houden. Vanuit de classificatie volgt de periodiciteit van het leveranciersgesprek:

<< afhankelijk van de keuze het andere niveau weghalen >>

Midden risico: regelmatig contract management overleg, minimaal 1x per jaar een leveranciersbeoordeling. Bij een op/aanmerking binnen de leveranciersbeoordeling wordt binnen 3 maanden een vervolgoverleg ingepland (afhankelijk van de grootte van het risico).

Hoog risico: frequent contract management overleg, wat ook geborgd kan worden binnen een operationeel, tactisch of strategisch overleg. Minimaal 1x per jaar een leveranciersbeoordeling. Bij een

¹ Dossier Afspraken en Procedures
Bijlage 9 - Agenda leveranciersgesprekken versie 2019

op/aanmerking binnen de leveranciersbeoordeling wordt binnen 3 maanden een vervolgoverleg ingepland (afhankelijk van de grootte van het risico).

Niveaus van communicatie

Er zijn drie niveaus van communicatie te onderscheiden in de relatie met leveranciers: strategisch, tactisch en operationeel. Elk niveau van communicatie heeft zijn eigen cyclus en deelnemende functionarissen. De betrokken functionarissen staan beschreven in het contract (paragraaf Overleg, Contactpersonen en Managementinformatie). Voor deze specifieke Model agenda is het communicatieniveau *strategisch / tactisch / operationeel* van toepassing:

<< afhankelijk van de keuze de andere niveaus weghalen >>

Strategisch

Overleg tussen de contracteigenaar van VRNHN en de leverancier om de ontwikkelingen bij beide organisaties te bespreken. Dit omvat nieuwe ontwikkelingen in de dienstverlening, andere strategische richting, wijzigingen contract etc. Dit type overleg vindt éénmaal per jaar of naar behoefte plaats.

Tactisch

Overleg tussen de contactpersoon van VRNHN en (bij ICT contracten) IM-ICT manager van VRNHN en de account- of delivery manager van de leverancier. Hier wordt besproken in hoeverre aan de SLA wordt voldaan, lopende projecten bij VRNHN die leverancier moet kennen, en de roadmap van projecten en aanpassingen in de dienstverlening bij VRNHN en de leverancier. Rapportage op overeengekomen KPI's en veiligheidsincidenten worden hier besproken. Twee of driemaandelijks overleg naar rato van omvang en belang van de dienstverlening door de leverancier voor VRNHN.

Operationeel

Overleg tussen bijvoorbeeld uitvoerende collega's, applicatiebeheerders / systeembeheerders van VRNHN en delivery manager, technische support van de leverancier. Hier staan incidenten die problemen zijn geworden en belangrijke wijzigingen op de agenda. Het gaat meer over de details van incidenten en wijzigingen met als doel e.e.a. op te lossen en te realiseren. Driewekelijks of tweemaandelijks overleg naar rato van omvang en belang van de dienstverlening door de leverancier voor VRNHN.

De tactische en operationele bespreking kan ook gecombineerd worden en in een frequentie plaatsvinden die past bij het belang van de dienstverlening door de leverancier voor VRNHN.

5. Agenda leveranciersgesprekken: ICT

De volgende agendapunten zullen worden besproken tijdens het overleg:

<< maak een keuze uit de lijst met onderwerpen voor agendering in tactisch en operationeel overleg, en licht deze toe per onderwerp: wat ga je specifiek bespreken?>>

1. SLA
 - a. Rapportages (SLR)
2. Continuïteit
 - a. Beschikbaarheid systemen
 - b. Verloop back-up
 - c. Planning periodieke restoretest
3. Projectplanning, implementaties nieuwe softwarepakketten + upgraden nieuwe versies.
4. Capaciteitsmanagement
5. Security

- a. Datalekken
- b. Autorisatielogging
- c. Incidenten bij leverancier
- 6. Review document afgesproken procedures (DAP)
 - a. Rollen / Contactpersonen
 - b. Overlegstructuur
 - c. Beheerprocessen
 - I. Service Management
 - II. Incident Management
 - III. Change Management
 - IV. Standaard wijzigingsverzoek
 - V. Niet-standaard wijzigingsverzoek
 - VI. Problem Management
 - VII. Configuratie Management
 - VIII. Patch Management
 - IX. Updates en upgrades
 - d. Response- en servicetijden
 - e. Standaard Service Window
 - f. Standaard Maintenance Window
 - g. Communicatieproces bij escalaties

In het schema op de volgende pagina staan de KPI's toegelicht.

<<< Op de volgende pagina is een voorbeeld geplaatst van aspecten waarover rapportage gevraagd kan worden aan leveranciers (SLR). Dit kan per leverancier en naar geleverde dienst vastgesteld worden. Maak hierin dus ook steeds een keuze >>

<< voorbeeld >>>

KPI	Item	Maximum waarde
Informatiebeveiliging incidenten	aantal openstaande beveiliging incidenten (per prioriteit)	n.v.t.
	aantal ingelegde beveiliging incidenten over afgelopen maand (per prioriteit)	n.v.t.
	aantal afgehandelde beveiliging incidenten over afgelopen maand (per prioriteit)	n.v.t.
	reactietijd	
	- prio 1	15 minuten
	- prio 2	30 minuten
	time-to-fix	
Security updates	- prio 1	1 uur
	- prio 2	2 uur
	voortgangsrapportage.	
	- Prio 1	doorlopend
	- Prio 2.	ieder uur
	aantal missende (Windows) security updates met classificatie "critical" / "high" tot 1 maand oud	0
	aantal producten met een bekende End-Of-Life binnen 6 maanden (java, adobe, windows)	n.v.t.
Virussen/spam	Aantal uitgegeven/vervangen/ingetrokken/verlopen beveiligingscertificaten	
	Aantal systemen met een bijgewerkte virusscanner	>99% op datum van rapporteren
	Aantal niet automatisch verwijderde virussen/malware/etc	
Accounts met hoge privilege (admins)	Aantal tegen gehouden	n.v.t.
	aantal toegekende "speciale rechten"	n.v.t.
	aantal ingetrokken "speciale rechten"	n.v.t.
	totaal aantal actieve "speciale rechten".	n.v.t.
	Aantal account (incl. lijst) die ge-excludeerd zijn van de default password policy.	n.v.t.
Kwetsbaarheden (maandelijks geautomatiseerde scan)	Aantal mislukte inlogpogingen van administrators (=incident)	<2 per maand per beheerder
	aantal kwetsbaarheden vanaf het internet met classificatie "critical" / "high".	0
	aantal kwetsbaarheden van systemen vanaf het interne netwerk met classificatie "critical" / "high";	0
Penetratietesten	laatste datum uitgevoerd externe (gateway) penetratietest;	Datum
	laatste datum uitgevoerde interne (LAN) pentest.	Datum
	Openstaande items vanuit de penetratietesten per risicoklasse	0 voor de klasse hoog
Backups	aantal mislukte backups na handmatige herstart.	0
Meldingen uit de IDS/IPS (digitaal inbraakalarm)	aantal pogingen met klasse "medium" en "high" risk.	n.v.t.

6. Agenda leveranciersgesprekken: levering en dienstverlening

De volgende agendapunten zullen worden besproken tijdens het overleg:

<< voorbeeld: definitieve inhoud zal tussen Partijen afgestemd worden >>

1. Kwaliteit
 - a. Kwaliteit geleverde producten of diensten
 - b. Kwaliteitsbeheersing algemeen
2. Geld (financiële informatie)
 - a. Geoffreerd / geaccepteerde prijs en meer/minderwerk
 - b. Prijs/Kwaliteitverhouding
 - c. Geleverde overzicht en inzicht in kosten en uitnutting
3. Risico's
 - a. Voorgestelde beheersmaatregelen
 - b. Overige verbetervoorstellen
 - c. Risicobeheersing in het algemeen
4. Organisatie
 - a. Organisatie leverancier
 - b. Aantal wijzigingen projectteam (bijv. bij implementaties, uitvoerend werk)
 - c. Pro-actieve, innovatieve en creatieve instelling
 - d. Klantvriendelijk, betrouwbaar, transparant en integer gedrag
5. Informatie
 - a. Tijdige levering documenten
 - b. Nakomen afspraken
 - c. Tijdig melden van problemen en komen met oplossingsrichting
 - d. Geleverd inzicht in actuele stand van zaken
6. Tijd
 - a. Tijdige oplevering conform planning / afspraken
 - b. Tijdig gehaalde mijlpalen (bijv. bij implementaties)

<< voorbeeld >>

KPI	Item	Maximum waarde
Kwaliteit	Kwaliteit geleverde producten of diensten Kwaliteitsbeheersing algemeen	
Geld	Geoffreerd / geaccepteerde prijs en meer/minderwerk Prijs/Kwaliteitverhouding Geleverde overzicht en inzicht in kosten en uitnutting	
Risico's	Voorgestelde beheersmaatregelen Overige verbetervoorstellen Risicobeheersing in het algemeen	
Organisatie	Organisatie leverancier Aantal wijzigingen projectteam (bijv. bij implementaties, uitvoerend werk) Pro-actieve, innovatieve en creatieve instelling Klantvriendelijk, betrouwbaar, transparant en integer gedrag	
Informatie	Tijdige levering documenten Nakomen afspraken Tijdig melden van problemen en komen met oplossingsrichting Geleverd inzicht in actuele stand van zaken	
Tijd	Tijdige oplevering conform planning / afspraken Tijdig gehaalde mijlpalen (bijv. bij implementaties)	