GEMEENTE TILBURG

Beleid “Extern beheer informatievoorziening”

Informatiebeveiliging en Privacy

Versiebeheer

Versie	Datum	Auteur	Status/Wijzigingen
0.1	21-10-2020	Marius van Oers	Memo met uitwerking van de voorwaarden en uitgangspunten extern beheer op onze informatievoorziening
0.2	21-10-2020	Terence van Gestel	Aanzet strategische memo "Extern beheer informatievoorziening"
0.3	1-11-2020	Terence van Gestel Laura Huijbregts Sanne van den Bosch	Bespreken eerste aanzet
0.4	23-11-2020	Piet Liebrecht Perry van Amelsvoort	Review vanuit Technisch Beheer
0.5	1-12-2020	Ronald Janssens	Akkoord
0.6	2-12-2020	Terence van Gestel	Checklist maatregelen toegevoegd
0.7	16-12-2020	Terence van Gestel	Vaststelling in strategische taakgroep informatiebeveiliging
0.8	26-01-2021	Terence van Gestel	Opmerkingen team Applicatiebeheer verwerkt
1.0	17-02-2021	Terence van Gestel	Vaststelling in MT afdeling INT

Aanleiding

De informatievoorziening van gemeente Tilburg wordt beheerd door interne en externe medewerkers. Onze informatievoorziening zelf transformeert steeds meer van een On Premise (lokale) naar een Cloud (Externe) omgeving. Deze strategische richting is uitgewerkt in een Cloud strategie.

Het beheer van onze informatievoorziening (zowel voor On Premise als Cloud) wordt steeds vaker uitbesteed aan externe partijen. Hierbij is het van belang dat er goede afspraken gemaakt worden over technische en organisatorische maatregelen om informatieveiligheid en privacy te waarborgen.

Dit document beschrijft de waarborgen die verwacht worden van een externe leverancier als deze (een deel van) onze informatievoorziening in beheer heeft.

Ons uitgangspunt is de Baseline Informatiebeveiliging Overheid (BIO). De BIO geeft kaders en richting op het gebied van organisatorische en technische waarborgen. Vanuit de BIO is het nemen van een aantal overheidsmaatregelen verplicht.

Het beleid van gemeente Tilburg is dat we rondom informatieveiligheid en de te nemen maatregelen dezelfde lijn volgen voor externe partijen en onderliggende dienstverlening als voor onze interne organisatie.

Definitie
Extern beheer zijn taken die niet door eigen medewerkers van gemeente Tilburg worden uitgevoerd. Hierbij gaat het om IT gerelateerde taken waaronder systeem- en netwerkbeheer, (technisch) applicatiebeheer, end user beheer en externe monitoring van bijv. IT diensten zoals een Firewall.

Verantwoordelijkheid

Het afdelingshoofd Informatietechnologie (INT) is verantwoordelijk voor het beleid "Extern beheer informatievoorziening". Hierbij gaat het beleid uit van organisatieafspraken waarbij de verantwoordelijkheid voor aanschaf en beheer van IT bij de afdeling INT ligt.

1. Algemene waarborgen

1.1 Baseline Informatiebeveiliging Overheid (BIO) als uitgangspunt;

Net zoals gemeente Tilburg hanteert een externe partij de BIO als normenkader voor informatiebeveiliging. De opdrachtnemer committeert zich in de offerte en overeenkomst aan de BIO. In een uitwerking specificeert de opdrachtnemer hoe men informatieveiligheid conform de BIO heeft geborgd. Een voorbeeld hiervan is dat de opdrachtnemer ISO 27001 gecertificeerd is.

1.2 Als (een medewerker van) de opdrachtnemer zich niet aan het beleid "extern beheer" houdt is dit een inbreuk op de onderliggende overeenkomst en kan gemeente Tilburg de overeenkomst per direct beëindigen. Eventuele (directe of indirecte) schade veroorzaakt door het niet nakomen van de afspraken kan worden verhaald op de opdrachtnemer.

2. Organisatorische waarborgen

2.1 ***Overeenkomst.***
Er is een overeenkomst afgesloten tussen de opdrachtgever en opdrachtnemer.
Deze overeenkomst beschrijft exact wat de dienstverlening inhoudt en adopteert de Gibit voorwaarden. Afwijkingen ten opzichte van de Gibit zijn duidelijk en onderbouwd beschreven. De overeenkomst is getoetst door team inkoop. Bij een langdurige (niet eenmalige) opdracht is de overeenkomst voorzien van een Service Level Agreement.

2.2 Verwerkersovereenkomst VWO.
Als er in de uitbesteding sprake is van "het verwerken van" persoonsgegevens wordt er een VWO gesloten. Hiervoor gebruiken we het slabloon van gemeente Tilburg. Beoordeling en goedkeuring van de VWO gebeurt door onze privacy adviseurs.

2.3 ***Geheimhouding.***
De opdrachtnemer bevestigt geheimhouding voor alle informatie die tijdens de opdracht verkregen en/of verwerkt wordt. De opdrachtnemer legt deze geheimhouding schriftelijk op aan de eigen medewerkers.

2.4 Verklaring Omtrent Gedrag (VOG).
Medewerkers van de opdrachtnemer die voor gemeente Tilburg werkzaamheden verrichten zijn specifiek voor het proces van deze werkzaamheden in bezit van een VOG. Deze VOG is niet ouder dan 3 jaar en in het bezit van de opdrachtnemer. Opdrachtnemer is zelf verantwoordelijk voor een juiste procesgang rondom de VOG.

2.5 ***Toepassen lokaal (informatiebeveiligings)beleid.***
Medewerkers van de opdrachtnemer vragen proactief naar lokale beleidsdocumenten (die relevant zijn voor het uitvoeren van de opdracht). Beleidsdocumenten worden toegepast in de uitvoering. Voorbeelden hiervan zijn: beleid op dataclassificatie, patchmanagement beleid, procesaanpak autorisaties en het wachtwoordbeleid.

2.6 ***Interne contactpersoon/buddy.***
Een externe medewerker heeft altijd een interne contactpersoon/buddy. Deze interne contactpersoon is op de hoogte van (geplande) werkzaamheden en eerste contactpersoon bij escalatie of calamiteiten. De interne opdrachtgever (= degene die de opdracht extern uitzet) is verantwoordelijk voor het koppelen van de buddy. Dit gaat in overleg met de teammanager of een adviseur van het betrokken IT team.

2.7 ***Toepassen van lokale beheerprocessen.***
Medewerkers van de opdrachtnemer maken voor het uitvoeren van hun werkzaamheden gebruik van onze beheerprocessen en documentatie. Als er van processen of documentatie moet worden afgeweken bespreekt de opdrachtnemer dit met de interne (gemeentelijke) contactpersoon. Afwijkingen worden met onderbouwing genoteerd. Een voorbeeld van een lokaal beheerproces is het Wijzigingsbeheerproces.

2.8 ***Individuele accounts.***

Medewerkers van de opdrachtnemer voeren werkzaamheden uit op basis van individuele accounts. Zo is altijd herleidbaar wie welke actie heeft uitgevoerd op onze omgeving. Een uitzondering hierop kan zijn dat een actie alleen vanuit een functioneel account kan worden uitgevoerd. In dat geval is er altijd een 4 ogen principe van toepassing en worden de activiteiten geregistreerd (zie hiervoor 3.6 logging). Individuele accounts en de onderliggende autorisatiegegevens zijn persoonlijk en NIET overdraagbaar. Het aanvragen en beëindigen van accounts is de verantwoording van de proceseigenaar (=afdelingshoofd of gemandateerd teammanager) "degene die de overeenkomst sluit met de opdrachtnemer".

3. Technische waarborgen

3.1 Veilige (beheer software).

De opdrachtnemer maakt voor het beheer van onze omgeving gebruik van onze beheer toepassingen. Als de opdrachtnemer eigen toepassingen wil of moet inzetten gaat dit in overleg met een IT architect en team technisch IT beheer van de opdrachtgever.

3.2 *Veilige verbindingen.*

De (internet) verbindingen van opdrachtnemer naar de informatievoorziening van gemeente Tilburg (intern of Cloud) voldoen aan standaarden op het gebied van informatiebeveiliging en zijn in lijn met de BIO. Denk hierbij aan VPN, Whitelisting, Netwerkzonering en Beveiligingscertificaten.

3.3 *Veilig inloggen.*

Externe toegang tot de informatievoorziening van de gemeente Tilburg gaat altijd op basis van Multi Factor Authenticatie. Als dit technisch of vanwege inrichting niet mogelijk is maakt men in overleg met team technisch IT beheer een risicoafweging en worden andere beveiligingstechnieken toegepast.

3.4 *Beheerde systemen.*

Beheerde systemen al dan niet intern of extern ontsloten die noodzakelijk zijn om de uitbestede dienstverlening te faciliteren worden veilig ontsloten (point-2-point VPN), staan in onze CMDB (inventarisatie) en kennen een interne (proces)eigenaar/verantwoordelijke. De interne opdrachtgever of proceseigenaar is verantwoordelijk voor het laten bijhouden van de CMDB. Het implementeren van beheer systemen gaat via ons wijzigingsproces.

3.5 *Minimaal benodigde toegangsrechten.*

Medewerkers van de opdrachtnemer krijgen toegangsrechten op basis van Least Privileges (minimaal noodzakelijk) om hun werkzaamheden te kunnen uitvoeren. Als werkzaamheden incidenteel zijn worden de accounts bij aanvang van de werkzaamheden vrijgegeven en na de werkzaamheden weer afgesloten. Als werkzaamheden of de opdracht structureel zijn blijven accounts tijdens de overeengekomen periode actief. Deze situatie is gelijk aan ons intern proces en hiermee onze eigen medewerkers.

3.6 *Logging van (beheer) werkzaamheden.*

Zowel toegang tot onze informatievoorziening als inhoudelijke beheeracties worden geregistreerd. Dit kan al dan niet (waar dit is ingericht) geautomatiseerd of via het Wijzigingsbeheerproces en binnen de applicatie Topdesk. Logbestanden worden beschermd volgens het beleid dataclassificatie en kunnen achteraf door interne medewerkers van de gemeente Tilburg worden geanalyseerd.

Logbestanden bevatten de volgende informatie:

Wie voert de wijziging uit;
Wat is er aangepast;
Wanneer is de wijziging uitgevoerd;
Waar is de wijziging uitgevoerd;
Waarom is de wijziging uitgevoerd;

Bijlage Checklist waarborgen

Naam aanbesteding:

Datum ingevuld:

Ingevuld door:

Maatregel	**Akkoord Ja/Nee**
Commitment opdrachtnemer aan Baseline Informatiebeveiliging Overheid (BIO) normenkader voor informatieveiligheid	
Getekende overeenkomst conform Gibit voorwaarden is aanwezig	
Getekende Service Level Agreement (SLA) is aanwezig	
Indien van toepassing: Getekende Verwerkersovereenkomst (VWO) is aanwezig	
Bevestiging Geheimhouding en Verklaring Omtrent Gedrag (VOG) medewerkers	
Interne contactpersoon/buddy aangewezen	
Waarborgen rondom gebruikersaccount geregeld	
Waarborgen rondom veilige (internet)verbindingen zijn geregeld	
Logging/Monitoring geregeld	