Gemeente Amsterdam

Uitgebreide Risicoanalyse Informatiebeveiliging en Privacy

Jij en je gezondheid - Voortgezet Onderwijs

Datum :27-03-2019
Projectnummer :-
Projectleider 5.1, 2, e 5.1, 2, e --> verantwoordelijk voor jaarlijks uitvoeren URA.
Opdrachtgever :JGZ en EGZ
Versie : 0.9
Auteur 5.1, 2, e 5.1, 2, e 5.1, 2, e 5.1, 2, e
Functie:IBC/TSO

Versiebeheer

Versies

Versie	Datum	Auteurs	Samenvatting van de wijzigingen
0.6	05-03-2018	5.1, 2, e 5.1, 2, e 5.1, 2, e	Bijlage B toegevoegd
0.7	06-03-2018	5.1, 2, e	Review en kleine opmaak aanpassingen
0.8	20-03-2018	5.1, 2, e	Wijzigingen 5.1, 2, e doorgevoerd en Ontwerp-, programmeer-, implementatie beheer/onderhoudsfouten toelichting ingevuld.
0.9	13-04-2018	5.1, 2, e 5.1, 2, e	Review
0.9B	18-05-2018	5.1, 2, e 5.1, 2, e 5.1, 2, e en 5.1, 2, e	Bespreekpunten doorgenomen. Liggen nog enkele vraagstukken open over wie precies verantwoordelijk is voor applicatie JEJG (wordt nieuwe constructie nu echt doorgevoerd? Is dan alleen EGZ nog verantwoordelijk voor applicatie?)
0.9C	05-02-2019	5.1, 2, e	De taakverdeling tussen JGZ en EGZ is gewijzigd ten opzichte van eerdere jaren. Voorstel voor aanpassen URA door 5.1, 2, e Opgestuurd ter controle naar 5.1, 2, e 5.1, 2, e en 5.1, 2, e
0.9 D	27-03-2019	5.1, 2, e	Voorgestelde aanpassingen 5.1, 2, e en 5.1, 2, e vewerkt. 5.1, 2, e geen verdere opmerkingen.

Goedkeuring

Versie	Datum	Naam

Ter informatie aan

Versie	Datum	Naam

.

Inhoud

1 Inleiding 5
1.1 Aanpak 5

2 Informatiesysteem in kaart brengen 6

3 Analyse dreigingen 7

4 Bepalen maatregelen 8

Bijlage A. Model om informatiesysteem in kaart te brengen 9

Bijlage B. Model om dreigingen in kaart te brengen 14

Bijlage C. Tabel voor bepalen effect dreigingen 14

Bijlage D: Dreigingen specifiek voor soorten informatiesystemen 25

Bijlage E: Model voor overzicht maatregeldoelstellingen 26

Bijlage F: Model voor detailoverzicht maatregeldoelstellingen 29

Bijlage G: Risico’s en bedreigingen 30

1 Inleiding

In het PPM proces is opgenomen dat voor elk informatiesysteem tijdens de definitiefase een verkorte risicoanalyse informatiebeveiliging wordt uitgevoerd. Wanneer hieruit volgt dat de beveiligingseisen beperkt zijn, kan worden volstaan met het invoeren van de maatregelen uit de baseline informatiebeveiliging van de gemeente Amsterdam. Wanneer de eisen boven een bepaalde grens uitstijgen moet ook een uitgebreide risicoanalyse worden uitgevoerd. Dit document beschrijft de wijze waarop de uitgebreide risicoanalyse wordt uitgevoerd, de tools die daarbij worden gebruikt etc.

Doelstelling van de uitgebreide risicoanalyse is om in kaart te brengen welke maatregelen moeten worden getroffen om het juiste niveau van beveiliging te realiseren.

1.1 Aanpak

De uitgebreide risicoanalyse volgt een quick scan aanpak om ervoor te zorgen dat op een pragmatische en effectieve manier de juiste zaken in kaart worden gebracht. Uitgangspunt is dat de verkorte risicoanalyse informatiebeveiliging volledig is uitgevoerd en dat de resultaten daarvan beschikbaar zijn.

In de verkorte risicoanalyse is de insteek het proces dat afhankelijk is van de informatievoorziening. In de uitgebreide risicoanalyse ligt de nadruk op de informatievoorziening die het proces ondersteunt. De maatregelen die worden opgeleverd omvatten wel het volledige scala van organisatie tot technologie.

De uitgebreide risicoanalyse bestaat uit 3 hoofdstappen:

1. Het in kaart brengen van de onderdelen van de informatievoorziening conform het MAPGOOD model.
2. Het in kaart brengen van de dreigingen die relevant zijn voor het te onderzoeken informatiesysteem, met per dreiging het potentiële effect en de kans op optreden.
3. Het vertalen van de meest relevante dreigingen naar maatregelen die moeten worden getroffen.

2 Informatiesysteem in kaart brengen

Inzicht in de informatievoorziening is nodig om in de volgende stap de bedreigingen goed in kaart te kunnen brengen. We gebruiken het MAPGOOD model om alle componenten van de informatievoorziening in kaart te brengen. In bijlage A is een template hiervoor opgenomen. Het template kan volledig worden ingevuld door de systeemeigenaar, met hulp van de functioneel beheerder en eventueel een technisch beheerder. Belangrijk is dat ieder onderdeel van MAPGOOD volledig in kaart wordt gebracht zodat alle onderdelen bekend zijn. De componenten hoeven daarbij niet in detail te worden beschreven. Daarnaast is belangrijk dat goed onderscheid wordt gemaakt tussen de zaken waar de systeemeigenaar direct voor verantwoordelijk is en de zaken die hij/zij heeft uitbesteed en daarom onder het element DIENST vallen.

De volgende werkwijze wordt gehanteerd:

- De systeemeigenaar en analist bespreken in 30 minuten de bedoeling van het MAPGOOD overzicht.
- De systeemeigenaar (geholpen door functioneel en technisch beheer) vult het overzicht in. Hier zijn naar verwachting maximaal 4 uren voor nodig.
- De systeemeigenaar en analist bespreken in 30 tot 60 minuten de invulling.

3 Analyse dreigingen

Op basis van een standaard dreigingen invullijst (zie bijlage B) worden samen met de systeemeigenaar de relevante bedreigingen in kaart gebracht waardoor verlies aan beschikbaarheid, integriteit of vertrouwelijkheid kan ontstaan. In deze sessie wordt per MAPGOOD component (bijvoorbeeld Mens) besproken wat het effect is van het “onjuist werken”, “(tijdelijk) niet werken” of “niet aanwezig zijn” (is er niet) van deze component.

De dreigingen worden in de vorm van incidenten verwoord en per incident is op een 3-puntsschaal (L, M, H) aangegeven hoe groot de invloed ervan is op werking van het informatiesysteem (de schade) en wat de kans is op het optreden van de betreffende dreiging. Op basis van een standaard tabel wordt bepaald wat het totale effect is (kans x schade). De tabel die hiervoor wordt gebruikt is opgenomen in bijlage C.

De volgende werkwijze wordt gehanteerd:

- De analist bereidt de bespreking voor door 1. Uit de standaard lijst (bijlage B) de dreigingen te schrappen die zeker niet relevant zijn voor het informatiesysteem en 2. Uit de applicatiespecifieke lijst (bijlage D) de dreigingen toe te voegen die mogelijk relevant zijn voor het informatiesysteem. Inspanning is circa 2 uren.
- De analist en systeemeigenaar (eventueel met functioneel beheerder) vullen het bijgestelde model dreigingen in. Daarbij geven zij voor iedere dreiging aan wat de kans van optreden is, wat de mogelijke schade is en geven hier een toelichting op. Doorlooptijd is al snel 4 uren, bij een complex systeem het dubbele.
- De analist werkt de invulling uit waarbij hij zorgt voor bepaling van kans x schade en leesbare en ter zake doende uitwerking van de toelichtingen. Op basis van de berekening van de kans x schade bepaalde hij welke dreigingen het meest relevant worden geacht. Inspanning is circa 4 uren.

4 Bepalen maatregelen

In deze stap worden de maatregelen bepaald die moeten worden getroffen om de dreigingen het hoofd te bieden die in de vorige stap als meest belangrijk zijn bepaald. De maatregelen worden daarbij geformuleerd op het niveau van doelstellingen om ervoor te zorgen dat bij de invulling over de tijd heen rekening kan worden gehouden met de stand van zaken op dat moment. Tevens kan hiermee een leverancier functioneel worden aangestuurd.

De volgende werkwijze wordt gehanteerd:

- De analist controleert of de dreigingen die niet “H” of “HH” zijn geclassificeerd inderdaad door de standaard baseline worden afgedekt. Inspanning is 1 a 2 uren.
- De analist vertaald de dreigingen naar maatregeldoelstellingen die moeten worden getroffen. Op basis van zijn ervaring, kennis van de baseline en kennis van het onderhavige proces en informatiesysteem vult hij het overzicht voor maatregeldoelstellingen in. Hierin zijn alle gegevens in één overzicht elkaar gebracht. Als het goed is zijn alleen bepaalde vakken ingevuld. Inspanning is 4 a 8 uren.
- De analist en de systeemeigenaar bespreken het overzicht om zeker te stellen dat de juiste vertaling van dreigingen naar maatregeldoelstellingen is gemaakt en voegen eventuele additionele zaken toe. Doorlooptijd 2 uren.
- De analist vertaald het overzicht maatregeldoelstellingen naar het detailoverzicht. Daarbij voegt hij per maatregeldoelstellingen relevante toelichtingen en voorbeeldmaatregelen toe. Inspanning is circa 4 uren.

In principe is de analyse hiermee afgerond. Het detailoverzicht met maatregeldoelstellingen wordt door systeem eigenaar en de coördinator IB besproken om vast te stellen hoe de implementatie wordt georganiseerd. Daarbij kan bijvoorbeeld worden gekozen voor alternatieve maatregelen, bepaalde risico’s te accepteren (gezien de benodigde maatregelen), maatregelen op centraal niveau (i.p.v. proces/informatiesysteem) te nemen etc.

Bijlage A. Model om informatiesysteem in kaart te brengen

Componenten

De inventarisatie van de componenten van een informatiesysteem wordt uitgevoerd aan de hand van de zogenaamde MAPGOOD componenten, MAPGOOD staat voor:

- **M**ens, de mensen die nodig zijn om het informatiesysteem te beheren en gebruiken.
- **A**pparatuur, de apparatuur die nodig is om het informatiesysteem te laten functioneren.
- **P**rogrammatuur, de programmatuur waaruit het informatiesysteem bestaat
- **G**egevens, de gegevens die door het systeem worden verwerkt
- **O**rganisatie, de organisatie die nodig is om het informatiesysteem te laten functioneren.
- **O**mgeving, de omgeving waarbinnen het informatiesysteem functioneert.
- **D**iensten, de externe diensten die nodig zijn om het systeem te laten functioneren.

Het is de bedoeling dat deskundigen - bijvoorbeeld de functioneel beheerder en technisch beheerder - de voornoemde componenten voor het eigen informatiesysteem beschrijven.

Invulling

Aan u het verzoek om voor een specifiek informatiesysteem de MAPGOOD componenten in kaart te brengen. Het gaat om invulling van de 2 rechterkolommen in de hierna opgenomen tabel. Voeg waar nodig nieuwe rijen in.

Aan het einde van dit document is een voorbeeld opgenomen dat als hulp kan dienen voor de invulling.

Bij de invulling moeten zowel de centrale als de decentrale onderdelen worden meegenomen. Decentraal betreft dit bijvoorbeeld gebruikers van een stadsdeel, de PC en infrastructuur die deze gebruiker nodig heeft, de gegevens en programmatuur die ter plaatse nodig zijn, het lokale beheer ter plaatse etc.

INVULLING MAPGOOD TBV INFORMATIESYSTEEM
Jij en je gezondheid

Component	**Onderdelen**	**Invulling**
Mens (Welke mensen gebruiken het systeem?)	Directe gebruikers	Leerlingen (LL) Jeugdartsen en -verpleegkundigen (JGZ) Doktersassistentes (JGZ)
	Indirecte gebruikers	JGZ-planbureau Databeheer Onderzoekers
	Systeembeheer	Functioneel beheer JGZ Functioneel beheer JEJG
	Technisch beheer	Technisch beheer I&A
Apparatuur (Welke apparatuur kent het systeem?)	Applicatie Server	
	Database server	
	PC, tablet of smartphone voor LL	Computers, tablets en/of smartphones op school.
	PC of tablet voor gebruikers JGZ	Computers en/of tablets directe gebruikers en ondersteuners (op eigen locaties).
	PC voor functioneel beheer JGZ en functioneel beheer JEJG	Computer van functioneel beheer JGZ en computer van functioneel beheer JEJG op GGD
	PC voor technisch beheer	Computer van I&A op GGD
Programmatuur (Welke programmatuur kent het systeem?)	Windows, PHP (frontend), MAGIC (backend)	
Gegevens (Welke gegevens kent het systeem?)	Schoolgegevens	Adres, contactgegevens, website, klassen.
	LL persoonsgegevens	BSN, voornaam, tussenvoegsel, achternaam, geboortedatum, postcode, school, klas, schoolniveau, gezinssituatie. E-mailadres voor het versturen van het persoonlijk profiel (optioneel), mobiel nummer (optioneel)
	LL antwoorden en uitslagen screeningsvragenlijsten	Sociaal-medische en sociaal-emotionele gegevens.
	LL antwoorden en uitslagen nader diagnostisch onderzoek	Sociaal-medische en sociaal-emotionele gegevens
	JGZ gegevens	Voornaam, achternaam, e-mailadres, 06-nummer, scholen binnen de eigen regio waar hij/zij zorg voor draagt.
	Databeheer gegevens	Voornaam, achternaam, e-mailadres, 06-nummer, regio waar hij/zij databeheer voor verzorgt.

	Functioneel beheer JGZ gegevens	Voornaam, achternaam, e-mailadres, 06-nummer, regio waar hij/zij functioneel beheerfunctie voor verzorgt.
	Functioneel beheer JEJG gegevens	Voornaam, achternaam, e-mailadres, 06-nummer.
	Technisch beheer gegevens	Voornaam, achternaam, e-mailadres, 06-nummer.
	Autorisatie gegevens	Gegevens omtrent de autorisatie die medewerkers hebben om met de applicatie te mogen werken.
	Log gegevens	Gegevens die het informatiesysteem opslaat mbt de transacties die worden uitgevoerd.
Organisatie (Welke organisatieonderdelen hebben met het systeem te maken?)	Gebruikersorganisatie JGZ	De organisatie rond de functioneel gebruikende JGZ.
	Organisatie JGZ-ondersteuning	De organisatie rond de planning van inzet JEJG binnen JGZ.
	Functioneel beheer organisatie JGZ	De organisatie rond functioneel beheer JGZ.
	Technisch beheer organisatie I&A	De organisatie rond technisch beheer.
	Functioneel beheer organisatie JEJG	De organisatie rond functioneel beheer JEJG.
Omgeving (Welke fysieke omgevingen zijn voor het systeem?)	Serverruimte	Hier staan de centrale servers.
	Werkplekken JGZ	Hier werken jeugdartsen en jeugdverpleegkundigen. Dit kan zijn op een OKT-locatie maar ook met laptop/tablet in ruimte op school.
	Computerlokalen op school	Hier vullen leerlingen de vragenlijst in.
	Buitenschoolse locaties van LL	Hier kunnen leerlingen hun persoonlijk profiel met uitslag en tips nogmaals inzien.
	Werkplek JGZ-ondersteuners	Hier werken medewerkers JGZ-planbureau.
	Werkplek functioneel beheer JGZ en functioneel beheer JEJG	Hier werkt functioneel beheer JGZ en functioneel beheer JEJG. Dit is op de GGD NA.
	Technisch applicatiebeheer	Hier werkt technisch beheer. Dit is op de GGD NA.
Diensten (Welke diensten horen bij het systeem?)	Technisch beheer besturings-systemen, netwerkinfrastructuur, netwerkdiensten.	Uitgevoerd door I&A.
	Beheer doorontwikkeling systeem JEJG	Uitgevoerd door Itforcare en functioneel beheer JEJG.
	Beheer systeem JEJG (vragenlijsten, gezondheidsboodschappen).	Uitgevoerd door functioneel beheer JEJG.
	Beheer gebruik JEJG (autorisaties, schoolprofielen).	Uitgevoerd door functioneel beheer JGZ.
	Koppelen JEJG met JGZ-kinddossier Kidos voor uitwisselen gegevens.	Geactiveerd door JGZ planbureau en geautomatiseerd uitgevoerd.

	Leveren van databestand voor onderzoek.	Uitgevoerd door databeheer JGZ
	Gebruikersovereenkomst te leveren diensten (product- en dienstenovereenkomst) aan externe gebruikers. Verwerkersovereenkomst voor het bewerken van aangeleverde data.	Uitgevoerd door projectleider JEJG.

VOORBEELD: MAPGOOD invulling (invulling is willekeurig)

Component	**Onderdelen**	**Invulling**
Mens (welke mensen gebruiken het systeem?)	Directe gebruikers	*Zorgbegeleider XXX* *Medewerkers Zorgregistratie XXX* *Medewerkers xxx*
	Indirecte gebruikers	*Gebruikers stadsdelen xxx* *Gebruikers front office organisatie xxx* *Gebruikers afnemer xxx*
	Functioneel applicatiebeheerder	*Functioneel beheerders afdeling "Hulpvraag",* 5.1, 2, e *en* 5.1, 2, e
	3e lijns applicatie support	*Is uitbesteed bij xxx*
	Technisch applicatiebeheer	*Is uitbesteed bij xxx*
	Systeembeheer	*Is uitbesteed bij xxx*
Apparatuur (Welke apparatuur kent het systeem?)	xxx presentatie server	*Server xxx in serverruimte xxx*
	xxx database server	*Server xxx in serverruimte xxx*
	Lokale PC voor script	*Computer* 5.1, 2, e
	Werkplekken van gebruikers	*Intern de standaard XXX werkplekken* *Extern eigen werkplekken*
Programmatuur (Welke programmatuur kent het systeem?)	Microsoft besturingssysteem (.NET)	Software op presentatie server
	Internet Information Server (IIS) van MicroSoft	Software op presentatie server
	Oracle Database v 9	*Software op database server*
	MicroSoft Reporting Services	*Software op presentatie server*
	Maatwerkbeveiligingscomponenten (SSS)	*Software op server xxx*
Gegevens (Welke gegevens kent het systeem?)	Zorgexploitatie gegevens	*Gegevens van mogelijke kosten en opbrengsten van (toekomstige) xxx*
	Object gegevens	*xxx*
	Klantgegevens	

BENOEM ALLE GEGEVENS SOORTEN!	Autorisatiegegevens	*Gegevens omtrent de autorisatie die medewerkers hebben om met de applicatie te mogen werken.*
	Log gegevens	*Gegevens die het informatiesysteem opslaat mbt de transacties die worden uitgevoerd.*
Organisatie (Welke organisatieonderdelen hebben met het systeem te maken?)	Beheerorganisatie	*De organisatie rond de functioneel beheerders*
	Gebruikersorganisatie	*De organisatie rond de gebruikers*
Omgeving (Welke fysieke omgevingen zijn voor het systeem?)	Serverruimte	*Hier staan de centrale servers*
	Werkplekken XXX	*Hier zitten de gebruiker en functioneel beheerders en staan de PC's en printers.*
	Technisch applicatiebeheer	*Door dienstverlener*
Diensten (Welke diensten horen bij het systeem?)	Technisch systeembeheer (besturingssystemen, databases etc.)	*Uitgevoerd door xxx*
	Netwerkinfrastructuur, netwerkdiensten (Inloggen, SSS, …), werkplekken, printers etc.	*Uitgevoerd door xxx*
	Onderhoudscontract en strippenkaart	*Bij xxx*

Bijlage B. Model om dreigingen in kaart te brengen

Component	Incident	Onderdelen	Schade (L,M,H)	Kans (L,M,H)	Totaal (L,M,H)	Toelichting (gevolgen etc.)
Mens						
• Functioneert onjuist • Niet aanwezig • Niet in dienst	Wegvallen • Voorzienbaar (ontslag, vakantie) • Onvoorzienbaar (ziekten, overlijden, ongeval, staking)	Leerlingen	L	M	L	Leerling wordtt opnieuw benaderd of wordt gemist.
		Jeugdartsen en -vpk	M	M	M	Invaller nodig of opnieuw inplannen waardoor vertraging.
		Databeheer Onderzoekers	L	L	L	Vervanger nodig.
		JGZ-planbureau	M	M	M	Vervanger nodig of proces afname vragenlijst loopt vast.
		Functioneel beheer JGZ	H	M	H	Stagneert functioneren systeem JEJG.
		Functioneel beheer JEJG	H	L	M	Stagneert doorontwikkeling systeem JEJG.
		Technisch beheer I&A	H	M	H	Stagneert functioneren systeem JEJG.
	Onopzettelijk foutief handelen • Onkunde, slordigheid • Foutieve procedures • Complexe foutgevoelige bediening • Onzorgvuldige omgang met wachtwoorden • Onvoldoende kennis/training	Leerlingen Jeugdartsen en -vpk	L H	H L	M M	Leerlingen snappen vaak niet alle vragen goed en kunnen slordig zijn. Kans op schade is niet hoog omdat er waar nodig nog een gesprek volgt en ook andere bronnen worden geraadpleegd. Foutief handelen van JGZ professional kan zeer schadelijk zijn, kans hierop is klein door overzichtelijkheid van het systeem.
		Databeheer	H	M	H	Persoonsgegevens kunnen op een verkeerder manier worden verwerkt.
		Onderzoekers	H	L	M	Fouten in analyses en rapportages.
		JGZ-planbureau	H	M	H	Ernstige gevolgen voor afname vragenlijsten: risico op foutieve LL-lijst en praktische problemen met afname.
		Functioneel beheer JGZ	H	L	M	Op alle fronten problemen van functioneren systeem JEJG. Back-up is geregeld.
		Functioneel beheer JEJG	H	L	M	Op alle fronten problemen van functioneren systeem JEJG. Back-up is geregeld.
		Technisch beheer I&A	H	M	H	Problemen met systeem, beheer I&A niet elke werkdag goed bereikbaar.

Component	Incident	Onderdelen	Schade (L,M,H)	Kans (L,M,H)	Totaal (L,M,H)	Toelichting (gevolgen etc.)
	Opzettelijk foutief handelen • Niet werken volgens voorschriften/procedures • Fraude/diefstal/lekken van informatie • Ongeautoriseerde toegang met account van medewerker met hogere autorisaties	Leerlingen Jeugdartsen en -vpk	L H	H L	M M	Leerlingen: onbruikbare uitkomsten screening en nader onderzoek. JGZ: onrechtmatig gebruik van JEJG mogelijk strafbaar.
		Databeheer	H	L	M	
		Onderzoekers	H	L	M	
		JGZ-planbureau	H	L	M	
		Functioneel beheer JGZ	H	L	M	
		Functioneel beheer JEJG	H	L	M	
		Technisch beheer I&A	H	L	M	
Apparatuur						
• Functioneert onjuist • Stoort • Gaat verloren of raakt ernstig beschadigd	Spontaan technisch falen • Veroudering/slijtage • Storing • Ontwerp/fabricage/installatie-onderhouds fouten	Server	H	M	H	Er zijn voorbeelden bekend van matige performance.
		Database server	H	M	H	Er zijn voorbeelden bekend van matige performance.
		PC of tablet op school voor LL	L	L	LL	Voldoende uitwijkmogelijkheden bij problemen.
		PC of tablet van gebruikers JGZ, JGZ planbureau	L	L	LL	Voldoende uitwijkmogelijkheden bij problemen.
		PC voor functioneel beheer JGZ	L	L	LL	Voldoende uitwijkmogelijkheden bij problemen.
		PC voor functioneel beheer JEJG	L	L	LL	Voldoende uitwijkmogelijkheden bij problemen.
		PC voor technisch beheer	L	L	LL	Voldoende uitwijkmogelijkheden bij problemen.
	Technisch falen door externe invloeden • Stroomuitval • Slechte klimaatbeheersing • Nalatig onderhoud door schoonmaak	Server	H	L	M	
		Database server	H	L	M	
		PC of tablet op school voor LL	L	L	LL	
		PC of tablet van gebruikers JGZ,	L	L	LL	

Component	Incident	Onderdelen	Schade (L,M,H)	Kans (L,M,H)	Totaal (L,M,H)	Toelichting (gevolgen etc.)
	• Natuurgeweld • Diefstal/schade	JGZ-planbureau				
		PC voor functioneel beheer JEJG	L	L	LL	
		PC voor functioneel beheer JGZ	L	L	LL	
		PC voor technisch beheer	L	L	LL	
	Menselijk handelen/falen • Installatiefout • verkeerde instellingen • Bedieningsfouten • Opzettelijke aanpassingen/sabotage • Beschadiging/vernieling • Verlies/Diefstal (o.a. verlies USB sticks) • Verwijdering van onderdelen waardoor storingen ontstaan	Server	H	L	M	Door systeem van test en hertest kunnen fouten worden hersteld voor productie.
		Database server	H	L	M	Door systeem van test en hertest kunnen fouten worden hersteld voor productie.
		PC of tablet op school voor LL	L	L	LL	
		PC of tablet gebruikers JGZ, JGZ-planbureau	L	L	LL	
		PC voor functioneel beheer JEJG	L	L	LL	
		PC voor functioneel beheer JGZ	L	L	LL	
		PC voor technisch beheer	L	L	LL	
Programmatuur						
• Functioneert onjuist • Loopt vast of vertraagde uitvoering • Gaat verloren of raakt ernstig beschadigd	Nalatig menselijk handelen • Ontwerp-, programmeer-, implementatie beheer/onderhoudsfouten • Introductie van virus e.d. door gebruik van ongescreende programma's • Gebruik van de verkeerde versie van programmatuur • Slechte documentatie	Ontwerp-, programmeer-, implementatie beheer/onderhoudsfouten	H	M	H	In het verleden is acceptatie omgeving per ongeluk uitgerold op productie. Naar aanleiding hiervan zijn acties ondernomen en is releasemanagement opgesteld. Dat wordt nu bij elke release toegepast. Concreet houdt dit in: - Er worden zo min mogelijk releases gepland. - Vanuit Itforcare 2 ontwikkelaars betrokken die elkaar controleren. - Releases worden nauwkeurig afgestemd met alle betrokkenen. - Releases vinden plaats in het weekend of na kantooruren (17.00). - Wanneer een release plaatsvindt worden verbeterpunten en basisfunctionaliteiten voor

Component	Incident	Onderdelen	Schade (L,M,H)	Kans (L,M,H)	Totaal (L,M,H)	Toelichting (gevolgen etc.)
						kantoortijd (08.30) getest door functioneel beheer JEJG. - In de acceptatie-omgeving staat nu 'acceptatie', zodat je in één oogopslag ziet of je in de acceptatie-omgeving zit of in de productie-omgeving.
		Introductie van virus e.d. door gebruik van ongescreende programma's	H	L	M	Defense in depth
		Slechte documentatie	M	M	M	
		Gebruik van de verkeerde versie van programmatuur	H	L	M	Door systeem van test en hertest kunnen fouten worden hersteld voor productie.
	Onopzettelijk menselijk handelen • Fouten door niet juist volgen van procedures • Installatie van malware en virussen door gebruik van onjuiste autorisaties	Fouten door niet juist volgen van procedures	H	L	M	
		Installatie van malware en virussen door gebruik van onjuiste autorisaties	H	L	M	
	Opzettelijk menselijk handelen • Manipulatie voor of na ingebruikname • (ongeautoriseerde) functieverandering en/of toevoeging • Installatie van virussen, Trojaanse paarden e.d.. • Kapen van autorisaties van collega's • Illegaal kopiëren van programmatuur • Oneigenlijk gebruik of privé-gebruik van bedrijfs programmatuur	Allen	H	L	M	VOG, de ambtseed.
	Technische fouten/mankementen • Fouten in code programmatuur die de werking		H	L	M	VOG, de ambtseed.

Component	Incident	Onderdelen	Schade (L,M,H)	Kans (L,M,H)	Totaal (L,M,H)	Toelichting (gevolgen etc.)
	verstoren • Achterdeuren in programmatuur voor (onbevoegde) toegang • Bugs/fouten in code die tot exploits kunnen leiden					
	Organisatorische fouten • Leverancier gaat failliet • Geen goede afspraken met leverancier	Geen goede afspraken met leverancier	H	M	H	Door interne samenwerking worden wensen en noodzaak niet altijd goed ingeschat. Belangrijk om de relatie tussen team JEJG en Itforcare formeel te houden. Gelijk aan relatie met klant buiten de GGD/gemeente.
Gegevens						
• Worden onterecht ontsloten • Zijn tijdelijk ontoegankelijk • Gaan verloren	• Diefstal/zoekraken/lekken • Beschadiging door verkeerde behandeling • Niet overeenkomende bestandformaten • Foutieve of geen versleuteling • Foutieve of vervalste identificatie van ontvangers om aan gegevens te komen	Geen versleuteling	H	L	M	
		Foutieve of vervalste identificatie van ontvangers om aan gegevens te komen	H	L	M	
		E-mail met uitslag wordt door andere leerling geopend	H	L	M	
	• Ongeautoriseerde toegang door onbevoegden (hackers/hosters) • Ongeautoriseerde wijziging of verwijdering van gegevens (hacking)	Ongeautoriseerde toegang door onbevoegden (hackers/hosters)	H	L	M	
		Ongeautoriseerde wijziging of verwijdering van gegevens (hacking)	H	L	M	
	Via apparatuur • Fysieke schrijf- of leesfouten • Onvoldoende toegangsbeperking tot apparatuur • Fouten in interne geheugens		H	L	M	

Component	Incident	Onderdelen	Schade (L,M,H)	Kans (L,M,H)	Totaal (L,M,H)	Toelichting (gevolgen etc.)
	• Aftappen van gegevens					
	Via programmatuur • Foutieve of gemanipuleerde programmatuur • Doorwerking van virussen/malware	Afbreken van verwerking	H	L	M	
	Via personen • (On)opzettelijke foutieve gegevensinvoer, -verandering of –verwijdering van data • Onbevoegde toegang door onbevoegden • Onbevoegd kopiëren van gegevens • Meekijken over de schouder door onbevoegden • Onzorgvuldige vernietiging • Niet toepassen clear screen/clear desk • Aftappen (draadloos) netwerk door onbevoegden (telewerk situaties) • Oneigenlijk gebruik van autorisaties • Toegang verschaffen tot d.m.v. identiteitsfraude of social engineering	(On)opzettelijke foutieve gegevensinvoer, -verandering of –verwijdering van data	H	L	M	
		Toegang door onbevoegden	H	L	M	
		Onbevoegd kopiëren van gegevens	H	L	M	
		Meekijken over de schouder door onbevoegden	H	M	H	Redelijk eenvoudig om bij een ingelogde gebruiker over de schouder mee te kijken. Door overzicht in de applicatie is snel informatie te zien.
		Onzorgvuldige vernietiging	H	L	M	
		Aftappen (draadloos) netwerk door onbevoegden (telewerk situaties)	H	L	M	
		Oneigenlijk gebruik van autorisaties	H	M	H	Mensen die uit dienst gaan worden niet altijd actief gemeld bij functioneel beheer JGZ.
		Toegang verschaffen tot informatie d.m.v. identiteitsfraude of social engineering	H	M	H	

Component	Incident	Onderdelen	Schade (L,M,H)	Kans (L,M,H)	Totaal (L,M,H)	Toelichting (gevolgen etc.)
Organisatie						
• Werkt niet volgens vastgestelde uitgangspunten • Reorganiseert • Fuseert of wordt opgeheven	Gebruikersorganisatie • Mismanagement • Gebrekkige toedeling taken, bevoegdheden, verantwoordelijkheden • Onduidelijke of ontbrekende gedragscodes • Afwezige, verouderde of onduidelijke handboeken / • systeemdocumentatie / werkprocedures/ gebruiksinstructies • Onvoldoende interne controle • Onvoldoende toetsing op richtlijnen • Onvoldoende of geen contractbeheer • Ontbrekende of onduidelijke SLA's • Gebrekkige doel/middelen beheersing	Mismanagement	H	L	M	
		Gebrekkige toedeling taken, bevoegdheden, verantwoordelijkheden	M	M	M	
		Onduidelijke of ontbrekende gedragscodes	H	L	M	
		Afwezige, verouderde of onduidelijke handboeken /	L	L	LL	
		systeemdocumentatie / werkprocedures/ gebruiksinstructies	L	L	LL	
		Onvoldoende interne controle	L	L	LL	
		Onvoldoende toetsing op richtlijnen	H	L	M	
		Onvoldoende of geen contractbeheer	H	L	M	Met elke regio die gebruik maakt van JEJG wordt een product- en dienstenovereenkomst en een verwerkersovereenkomst afgesloten.
		Ontbrekende of onduidelijke SLA's	H	L	M	De SLA wordt elk jaar door de projectleider JEJG gecheckt en waar nodig aangepast.
	Beheerorganisatie • Gebrekkig beleid betreffende beheer • Onvoldoende kennis of capaciteit	Gebrekkig beleid betreffende beheer	H	L	M	
		Onvoldoende kennis of	H	L	M	

Component	Incident	Onderdelen	Schade (L,M,H)	Kans (L,M,H)	Totaal (L,M,H)	Toelichting (gevolgen etc.)
	• Onvoldoende kwaliteitsborging • Onvoldoende beheer van systemen en middelen (ICT Atlas)	capaciteit				
		Onvoldoende kwaliteitsborging	H	L	M	
		Onvoldoende beheer van systemen en middelen (ICT Atlas)	H	L	M	
	Ontwikkelingsorganisatie • Slecht projectmanagement • Niet volgen van projectenkalender of PPM • Geen ontwikkelrichtlijnen en/of – procedures • Er worden geen methoden/technieken gebruikt • Gebrek aan planmatig werken	Slecht projectmanagement	M	L	L	
		Niet volgen van projectenkalender of PPM	M	L	L	
		Geen ontwikkelrichtlijnen en/of – procedures	M	L	L	
		Er worden geen methoden/technieken gebruikt	L	L	LL	
		Gebrek aan planmatig werken	M	L	L	
Omgeving						
• Is toegankelijk voor ongeautoriseerden • Is beschadigd • Is verwoest of ernstig beschadigd	Huisvesting • Ongeautoriseerde toegang tot gebouw(en) • Diefstal op werkplekken • Gebreken in ruimtes, waardoor kans op insluiping/inbraak • Onvoldoende fysieke voorzieningen om te vluchten of in te grijpen tijdens geweldsdreigingen/conflicten met klanten	Ongeautoriseerde toegang tot gebouw(en)	H	L	M	
		Diefstal op werkplekken	M	L	L	
		Gebreken in ruimtes, waardoor kans op insluiping/inbraak	H	L	M	
		Onvoldoende fysieke voorzieningen om te vluchten of in te grijpen tijdens geweldsdreigingen/conflicten met klanten	M	L	L	
	Nutsvoorzieningen • Uitval van elektriciteit, water, telefoon	Uitval van elektriciteit, water, telefoon	H	L	M	

Component	Incident	Onderdelen	Schade (L,M,H)	Kans (L,M,H)	Totaal (L,M,H)	Toelichting (gevolgen etc.)
	• Wateroverlast door lekkage, bluswater • Uitval van licht-, klimaat-, sprinklerinstallatie	Wateroverlast door lekkage, bluswater	H	L	M	
		Uitval van licht-, klimaat-, sprinklerinstallatie	H	L	M	
	Buitengebeuren • Natuurgeweld (overstroming, blikseminslag, storm, aardbeving etc) • Overig geweld (oorlog, terrorisme, brandstichting, inbraak, neerstortend vliegtuig) • Blokkade/staking • Onveilige, geblokkeerde, vluchtwegen bij 5.1, 2, e	Natuurgeweld (overstroming, blikseminslag, storm, aardbeving etc)	H	L	M	
		Overig geweld (oorlog, terrorisme, brandstichting, inbraak, neerstortend vliegtuig	H	L	M	
		Blokkade/staking	H	L	M	
		Onveilige, geblokkeerde, vluchtwegen bij 5.1, 2, e	H	L	M	
Diensten						
• Worden niet volgens afspraak geleverd • Tijdelijk niet te leveren • Definitief niet meer te leveren	**Diensten worden niet conform afspraak geleverd** • Slecht opgeleid personeel • Groot personeelsverloop • Onvoldoende capaciteit in personeel • Valse verklaringen over certificeringen • Onvoldoende of geen kwaliteitsborging • Personeel voldoet niet aan eisen zoals geldig VOG en geheimhoudingsverklaringen • Voert wanbeheer, slordigheden in beheersactiviteiten • Werkt niet conform ITIL of BiSL principes • Maakt misbruik van toevertrouwde gegevens, applicaties en documentatie	Slecht opgeleid personeel	H	L	M	
		Groot personeelsverloop	H	L	M	
		Onvoldoende capaciteit in personeel	H	L	M	Bij Itforcare zijn 3 medewerkers bekend met JEJG: 5.1, 2, e 5.1, 2, e en 5.1, 2, e
		Valse verklaringen over certificeringen	H	L	M	
		Onvoldoende of geen kwaliteitsborging	H	L	M	
		Personeel voldoet niet aan eisen zoals geldig VOG en geheimhoudingsverklaringen				NVT. Binnen de gemeente Amsterdam wordt alleen maar personeel aangenomen met een geldig VOG. Dit geldt ook voor de medewerkers van Itforcare.

Component	Incident	Onderdelen	Schade (L,M,H)	Kans (L,M,H)	Totaal (L,M,H)	Toelichting (gevolgen etc.)
	• Houdt zich niet aan functiescheiding • Maakt gebruik van te zware autorisatie, niet functiegebonden					
		Voert wanbeheer, slordigheden in beheersactiviteiten	H	L	M	
		Werkt niet conform ITIL of BiSL principes	L	L	LL	
		Maakt misbruik van toevertrouwde gegevens, applicaties en documentatie	H	L	M	
		Houdt zich niet aan functiescheiding	H	L	M	
		Maakt gebruik van te zware autorisatie, niet functiegebonden	L	L	LL	
	Diensten dienstverlener tijdelijk niet beschikbaar • Levert diensten niet conform overeenkomst • Onderbreking dienstverlening door overname dienstverlener • Kan diensten tijdelijk niet uitvoeren door zaken buiten de eigen controle (stakingen ed.) • Past verkeerde prioriteiten toe in klantbejegening • Levert onvoldoende capaciteit voor een goede dienstverlening	Levert diensten niet conform overeenkomst	H	L	M	
		Onderbreking dienstverlening door overname dienstverlener				NVT, we kunnen niet overgenomen worden.
		Kan diensten tijdelijk niet uitvoeren door zaken buiten de eigen controle (stakingen ed.)	M	L	M	
		Past verkeerde prioriteiten toe in klantbejegening	H	L	M	
		Levert onvoldoende capaciteit voor een goede dienstverlening	H	L	M	
	Diensten dienstverlener definitief niet meer te leveren	Een dienstverlener gaat failliet	H	L	M	Een failliete gemeente heeft nog wel haar wettelijke bevoegdheden en bestuurlijke plichten maar niet meer de materiële middelen om iets voor elkaar te krijgen. En

Component	Incident	Onderdelen	Schade (L,M,H)	Kans (L,M,H)	Totaal (L,M,H)	Toelichting (gevolgen etc.)
	• Een dienstverlener gaat failliet • Opzegging diensten door dienstverlener					geen geld meer om medewerkers te betalen. Dat werkt natuurlijk niet. Daarom is er nog nooit een gemeente failliet verklaard. Toch kan het formeel wel – de minister van Justitie heeft dat bevestigd. Als een gemeente over lange tijd grote financiële tekorten op de begroting heeft, kan die gemeente het Rijk om extra geld uit het Gemeentefonds vragen. De gemeente levert haar financiële zelfstandigheid voor een deel in, en krijgt een zogenoemde Artikel 12-status. Artikel 12 is het 12e artikel uit de Financiële-verhoudingswet.
		Opzegging diensten door dienstverlener	H	L	M	

Bijlage C. Tabel voor bepalen effect dreigingen

		SCHADE		
		H	**M**	**L**
KANS	**H**	HH	H	M
	M	H	M	L
	L	M	L	LL

Bijlage D: Dreigingen specifiek voor soorten informatiesystemen

Om de uitvoering van de dreigingenanalyse efficiënter en effectiever te laten verlopen, bepaalt analyse van te voren welke dreigingen expliciet relevant zijn voor het onderhavige informatiesysteem. Deze bijlage beschrijft een aantal soorten informatiesysteem met de bijbehorende specifieke dreigingen.

NB: Dit overzicht is in ontwikkeling qua formulering en volledigheid van de dreigingen

Documentair informatiesysteem

- Documenten niet beschikbaar voor proces (grote afhankelijkheid centrale opslag)

Via het internet toegankelijk webbased informatiesysteem

- Lekken van gegevens door “hacker”
- Defacement van website
- Fraude a.g.v. door misbruik door “hackers”
- DDoS aanval op website

Basisregistratie

- Ongewenste verandering van gegevens bij conversie/ophalen gegevens

Financieel systeem

-

Personeelssysteem

-

Facilitair systeem

-

Ketensysteem

-

Systeem in de cloud

- Niet voldoen aan wet- en regelgeving omdat gegevens in de cloud staan
- Afhankelijkheid van cloud leverancier m.b.t. beschikbaarheid
- Toegangscontrole onvoldoende c.q. onbeheersbaar

Bijlage E: Model voor overzicht maatregeldoelstellingen

			BESCHIKBAARHEID opnemen eis en kleur in hoogte eis zetten	CONTINUITEIT opnemen eis en kleur in hoogte eis zetten	INTEGRITEIT opnemen eis en kleur in hoogte eis zetten	VERTROUWELIJKHEID opnemen eis en kleur in hoogte eis zetten	PRIVACY opnemen eis en kleur in hoogte eis zetten
			Opnemen motivatie voor de gestelde eis.	Opnemen motivatie voor de gestelde eis.	Opnemen motivatie voor de gestelde eis.	Opnemen motivatie voor de gestelde eis.	Opnemen motivatie de gestelde voor eis.
MAPGOOD IB-GEBIED	**MENS** Opnemen beschrijving MAPGOOD element MENS	**APPARATUUR** Opnemen beschrijving MAPGOOD element APPARATUUR	**PROGRAMMATUUR** Opnemen beschrijving MAPGOOD element PROGRAMMATUUR	**GEGEVENS** Opnemen beschrijving MAPGOOD element GEGEVENS	**ORGANISATIE** Opnemen beschrijving MAPGOOD element ORGANISATIE	**OMGEVING** Opnemen beschrijving MAPGOOD element OMGEVING	**DIENSTEN** Opnemen beschrijving MAPGOOD element DIENSTEN
IB-beleid en -plan							
Organisatie van IB							
Classificatie en beheer van informatie en bedrijfsmiddelen							
Personele beveiligingseisen				**Meekijken over de schouder door onbevoegden** Maatregel: Security awareness			

				Oneigenlijk gebruik van autorisaties Maatregel: Account reviews regelmatig plannen. Eens per half jaar. Daarnaast Aansluiten bij de uitdienst procedure van automatisering.			
				Toegang verschaffen tot d.m.v. identiteitsfraude of social engineering Maatregel: Security awareness			
Fysieke beveiliging							
Beheer van communicatie- en bedieningsprocessen	**Onopzettelijk foutief handelen JGZ-planbureau, Functioneel beheer JEJG, Functioneel beheer JGZ, Technisch beheer.** Maatregel: Documentatie. Het bijhouden, opstellen, verspreiden en naleven van procedures.		**Ontwerp-, programmeer, implementatie beheer/ onderhoudsfouten** Maatregel: - Releasemanagement toepassen. Er worden zo min mogelijk releases gepland. - Vanuit Itforcare 2 ontwikkelaars betrokken die elkaar controleren. - Releases worden				

			nauwkeurig afgestemd met alle betrokkenen. - Releases vinden plaats in het weekend of na kantooruren (17.00). - Wanneer een release plaatsvindt worden verbeterpunten en basisfunctionaliteiten voor kantoortijd (08.30) getest door functioneel beheer JEJG. - In de acceptatie-omgeving staat nu 'acceptatie', zodat je in één oogopslag ziet of je in de acceptatie-omgeving zit of in de productie-omgeving.				
Logische toegangsbeveiliging							
Ontwikkeling en onderhoud van systemen		**Voorbeelden bekend van matige performance.** Maatregel: wanneer (1) nieuwe regio's gebruik gaan maken van JEJG (zodat	**Geen goede afspraken met leverancier.** Maatregel: Interne leveranciers beoordeling blijven uitvoeren bij ontevredenheid klant.				

		aantal gebruikers toeneemt) of (2) de performance slechter lijkt dan voorheen voert Itforcare een performancetest uit en rapporteert uitkomsten aan projectleider JEJG.					
Continuïteit	**Wegvallen van Functioneel beheer JEJG, Functioneel beheer JGZ, Technisch beheer.** Maatregel: Documentatie up to date houden en job rotation.						
Naleving							

Bijlage F: Model voor detailoverzicht maatregeldoelstellingen

Informatie-beveiligingsgebied	Maatregeldoelstelling	Toelichting en voorbeeldenmaatregelen.	**Implementatiewijze (in te vullen door organisatie)**
IB-beleid en plan	MAATREGELDOELSTELLINGEN OVERNEMEN UIT OVERZICHT TABEL	OPNEMEN TOELICHTINGEN EN VOORBEELDMAATREGELEN	
Organisatie IB			
Classificatie en beheer van informatie en bedrijfsmiddelen			
Personele beveiligingseisen	Security awareness. Meekijken over schouder.	Gebruikers regelmatig op de hoogte brengen over op de gevaren op dit gebied. Dit kan door middel van het intranet of bijvoorbeeld awareness campagnes en trainingen.	Opnemen in scholing. Belang van waarborgen privacy leerlingen aan bod laten komen.
Personele beveiligingseisen	Security awareness. Toegang verkrijgen door identiteitsfraude/social engineering.	Gebruikers regelmatig op de hoogte brengen over op de gevaren op dit gebied. Dit kan door middel van het intranet of bijvoorbeeld awareness campagnes en trainingen.	Opnemen in scholing. Belang van waarborgen privacy leerlingen aan bod laten komen.
Personele beveiligingseisen	Account reviews regelmatig plannen. Eens per half jaar. Aansluiten bij de uitdienst procedure van automatisering.	Controleren bij alle accounts of de rechten nog kloppen. Zorgen d.m.v. een melding bij automatisering dat JEJG meeloopt in de uit-dienst procedure. Medewerkers die uit dienst gaan worden gemeld bij Functioneel applicatiebeheer JGZ. Accounts worden niet verwijderd, want je wil nog wel in de geschiedenis kunnen kijken. Maar alle scholen worden ontkoppeld, zodat medewerker geen toegang meer heeft tot leerlingen.	(1) Op basis van inactiviteit in systeem JEJG nagaan of gebruikers nog in dienst zijn en waar mogelijk accounts verwijderen. Lijst is opgevraagd bij Itforcare. 5.1, 2, e heeft overzicht gemaakt. 5.1, 2, e pakt dit verder op. 5.1, 2, e kijkt of dit in de toekomst bij secretariaat kan komen te liggen.

Informatie-beveiligingsgebied	Maatregeldoelstelling	Toelichting en voorbeeldenmaatregelen.	**Implementatiewijze (in te vullen door organisatie)**
			(2) Aansluiten bij 'uit dienst procedure' van JGZ. Wanneer een medewerker uit dienst gaat wordt dat gemeld via 5.1, 2, i @ggd.amsterdam.nl
Fysieke beveiliging			
Beheer van communicatie- en bedieningsprocessen	Documentatie. Het bijhouden, opstellen, verspreiden en naleven van procedures om onopzettelijk foutief handelen te voorkomen.	Hierdoor is iedereen op de hoogte van de procedures en wordt de kans op foutief handelen kleiner.	Filmpje voor planproces VO? Er is een filmpje voor JGZ-professionals ontwikkeld hoe te registeren in Kidos. 5.1, 2, e vraagt bij de werkgroep verbeteringen planproces VO na of het handig is ook een filmpje te ontwikkelen voor het planproces.
Beheer van communicatie- en bedieningsprocessen	Releasemanagement toepassen om Ontwerp-, programmeer-, implementatie beheer/ Onderhoudsfouten te voorkomen.	Door release management wordt de uitgave van nieuwe software overzichtelijker en wordt de kans op fouten verkleind.	- Er worden zo min mogelijk releases gepland. - Vanuit Itforcare 2 ontwikkelaars betrokken die elkaar controleren. - Releases worden nauwkeurig afgestemd met alle betrokkenen.

Informatie-beveiligingsgebied	Maatregeldoelstelling	Toelichting en voorbeeldenmaatregelen.	**Implementatiewijze (in te vullen door organisatie)**
			- Releases vinden plaats in het weekend of na kantooruren (17.00) - Wanneer een release plaatsvindt worden verbeterpunten en basisfunctionaliteiten voor kantoortijd (08.30) getest door Functioneel beheer JEJG. - In de acceptatie-omgeving staat nu ‘acceptatie’, zodat je in één oogopslag ziet of je in de acceptatie-omgeving zit of in de productie-omgeving.
Logische Toegangsbeveiliging			
Ontwikkeling en onderhoud van systemen	Interne leveranciers beoordeling blijven uitvoeren bij ontevredenheid klant over afspraken met leverancier.	Hierdoor blijft de interne leverancier scherp en kunnen ontevredenheden met meer daadkracht aangegeven worden.	Wanneer de samenwerking met Itforcare niet verloopt zoals gewenst leveranciersbeoordeling aanvragen bij5.1, 2, e

Informatie-beveiligingsgebied	Maatregeldoelstelling	Toelichting en voorbeeldenmaatregelen.	**Implementatiewijze (in te vullen door organisatie)**
			5.1, 2, e
	Wanneer (1) nieuwe regio's gebruik gaan maken van JEJG (zodat aantal gebruikers toeneemt) of (2) de performance slechter lijkt dan voorheen voert Itforcare een performancetest uit en rapporteert uitkomsten aan projectleider JEJG.	Afspraken maken met Itforcare dat in genoemde twee situaties een performancetest wordt gedaan en de uitkomsten worden gerapporteerd aan projectleider JEJG.	
Continuïteit	Documentatie up to date houden en job rotation om het wegvallen van functioneel en –technisch beheer te voorkomen.	Hierdoor zijn anderen in staat het werk over te nemen.	Functioneel beheer JEJG: 5.1, 2, e en 5.1, 2, e Functioneel beheer JGZ: 5.1, 2, e en 5.1, 2, e
Naleving			

Bijlage G: Risico's en bedreigingen.

In deze tabel zijn alleen de risico's opgenomen die niet geaccepteerd zijn door de data-eigenaar. Alle risico's beneden de H zijn automatisch geaccepteerd, zie bijlage B.

Bedreigingen per groep		Schade			Kans			Geaccepteerd risico	Maatregel? + nummer
Mensen	**Incident**	**H**	**M**	**L**	**H**	**M**	**L**	**Ja/Nee**	**Ja/Nee/Nr.**
Wegvallen	Voorzienbaar (ontslag, vakantie)	X				X		Nee	Ja
	Onvoorzienbaar (ziekten, overlijden, ongeval, staking)	X				X		Nee	Ja
								Nee	Ja
Onopzettelijke foutieve handelen	Onkunde, slordigheid	X				X		Nee	Ja
	Foutieve procedures	X				X		Nee	Ja
	Complexe foutgevoelige bediening	X				X		Nee	Ja
	Onzorgvuldige omgang met wachtwoorden	X				X		Nee	Ja
	Onvoldoende kennis/training	X				X		Nee	Ja
Opzettelijke foutieve handelen	Niet werken volgens voorschriften/procedures								
	Fraude/diefstal/lekken van informatie								
	Ongeautoriseerde toegang met account van medewerker met hogere autorisaties								

Apparatuur	Incident	H	M	L	H	M	L	Ja/Nee	Ja/Nee/Nr.
Spontaan technisch falen	Veroudering/slijtage								
	Storing								
	Ontwerp/fabricage/installatie-onderhouds fouten								
Technisch falen door externe invloeden	Stroomuitval								
	Slechte klimaatbeheersing								
	Nalatig onderhoud door schoonmaak								
	Elektromagnetische straling								
	Elektrostatische lading								
	Diefstal/schade								
Menselijk handelen/falen	Bedieningsfouten								
	Opzettelijke aanpassingen/sabotage								
	Beschadiging/vernieling								
	Verlies/Diefstal (o.a. verlies van USB sticks)								
	Verwijdering van onderdelen waardoor storingen ontstaan								
Programmatuur	**Incident**	**H**	**M**	**L**	**H**	**M**	**L**	**Ja/Nee**	**Ja//Nee/Nr**
Nalatig menselijk handelen	Ontwerp-, programmeer-, implementatie beheer/onderhoudsfouten	X				X		Nee	Ja
	Introductie van virus e.d. door gebruik van ongescreende programma's	X				X		Nee	Ja
	Gebruik van de verkeerde versie van programmatuur	X				X		Nee	Ja
	Slechte documentatie	X				X		Nee	Ja
Opzettelijk menselijk handelen	Manipulatie voor of na ingebruikname								
	(ongeautoriseerde) functieverandering en/of toevoeging								
	Installatie van virussen, Trojaanse paarden e.d..								
	Kapen van autorisaties van collega's								
	Illegaal kopiëren van								

	programmatuur								
	Oneigenlijk gebruik of privé-gebruik van bedrijfs programmatuur								
Onopzettelijk menselijk handelen	Fouten door niet juist volgen van procedures								
	Installatie van malware en virussen door gebruik van hoge autorisaties bijvoorbeeld door gebruik van admin account tijdens het browsen van websites.								
Technische fouten/mankementen	Fouten in code programmatuur die de werking verstoren								
	Achterdeuren in programmatuur voor (onbevoegde) toegang								
	Bugs/fouten in code die tot exploits kunnen leiden								
	Organisatorische fouten Geen goede afspraken met leverancier	X				X		Nee	Ja
Gegevens/data	**Incident**	**H**	**M**	**L**	**H**	**M**	**L**	**Ja/Nee**	**Ja/Nee/Nr.**
Via gegevensdragers (CD/DVD/ USB Sticks/ Harddisk/ Backups	Diefstal/zoekraken/lekken								
	Beschadiging door verkeerde behandeling								
	Niet overeenkomende bestandformaten								
	Foutieve of geen versleuteling								
	Foutieve of vervalste identificatie van ontvangers om aan gegevens te komen								
Via Cloud voorzieningen	Ongeautoriseerde toegang door onbevoegden (hackers/hosters)								
	Ongeautoriseerde wijziging of verwijdering van gegevens (hacking)								
Via apparatuur	Fysieke schrijf- of leesfouten								
	Onvoldoende toegangsbeperking tot apparatuur								
	Fouten in interne geheugens								

	Aftappen van gegevens								
Via programmatuur	Foutieve of gemanipuleerde programmatuur								
	Doorwerking van virussen/malware								
	Afbreken van verwerking								
Via personen	(On)opzettelijke foutieve gegevensinvoer, -verandering of –verwijdering van data								
	Onbevoegde toegang door onbevoegden (hackers ed via malware)								
	Onbevoegd kopiëren van gegevens								
	Meekijken over de schouder door onbevoegden	X				X		Nee	Ja
	Onzorgvuldige vernietiging (laten liggen op printer)								
	Net toepassen clear screen/clear desk								
	Aftappen (draadloos) netwerk door onbevoegden (telewerk situaties)								
	Oneigenlijk gebruik van autorisaties	X				X		Nee	Ja
	Toegang verschaffen tot d.m.v. identiteitsfraude of social enginering	X				X		Nee	Ja
	Onzorgvuldig vernietigen van gegevens								
Organisatie	**Incident**	**H**	**M**	**L**	**H**	**M**	**L**	**Ja/Nee**	**Ja/Nee/Nr.**
Gebruikersorganisatie	Mismanagement								
	Gebrekkige toedeling taken, bevoegdheden,								
	verantwoordelijkheden								
	Onduidelijke of ontbrekende gedragscodes								
	Afwezige, verouderde of onduidelijke handboeken /								
	systeemdocumentatie / werkprocedures/ gebruiksinstructies								
	Onvoldoende interne controle								
	Onvoldoende toetsing op richtlijnen								
	Onvoldoende of geen contractbeheer								

	Ontbrekende of onduidelijke SLA's								
	Gebrekkige doel/middelen beheersing								
Beheerorganisatie	Gebrekkig beleid betreffende beheer								
	Onvoldoende kennis of capaciteit								
	Onvoldoende kwaliteitsborging								
	Onvoldoende beheer van systemen en middelen (ICT Atlas)								
Ontwikkelingsorganisatie	Slecht projectmanagement								
	Niet volgen van projectenkalender of PPM								
	Geen ontwikkelrichtlijnen en/of – procedures								
	Er worden geen methoden/technieken gebruikt								
	Gebrek aan planmatig werken								
Omgeving	**Incident**	**H**	**M**	**L**	**H**	**M**	**L**	**Ja/Nee**	**Ja/Nee/Nr.**
Buitengebeuren	Natuurgeweld (overstroming, blikseminslag, storm, aardbeving etc)								
	Overig geweld (oorlog, terrorisme, brandstichting, inbraak, neerstortend vliegtuig, galactische oorlogsvoering)								
	Blokkade/staking								
	Onveilige, geblokkeerde, vluchtwegen bij 5.1, 2, e								
Nutsvoorzieningen	Uitval van elektriciteit, water, telefoon								
	Wateroverlast door lekkage, bluswater								
	Uitval van licht-, klimaat-, sprinklerinstallatie								
Huisvesting	Ongeautoriseerde toegang tot gebouw(en)								
	Diefstal op werkplekken								
	Gebreken in ruimtes, waardoor kans op insluiping/inbraak								

	Onvoldoende fysieke voorzieningen om te vluchten of in te grijpen tijdens geweldsdreigingen/conflicten met klanten								
Diensten	**Incident**	**H**	**M**	**L**	**H**	**M**	**L**	**Ja/Nee**	**Ja/Nee/Nr.**
Diensten dienstverlener definitief niet meer te leveren	Een dienstverlener gaat failliet								
	Opzegging diensten door dienstverlener								
Diensten dienstverlener tijdelijk niet beschikbaar	Levert diensten niet conform overeenkomst								
	Onderbreking dienstverlening door overname dienstverlener								
	Kan diensten tijdelijk niet uitvoeren door zaken buiten de eigen controle (stakingen ed.)								
	Past verkeerde prioriteiten toe in klantbejegening								
	Levert onvoldoende capaciteit voor een goede dienstverlening								
Diensten worden niet conform afspraak geleverd	Slecht opgeleid personeel								
	Groot personeelsverloop								
	Onvoldoende capaciteit in personeel								
	Valse verklaringen over certificeringen								
	Onvoldoende of geen kwaliteitsborging								
	Personeel voldoet niet aan eisen zoals geldig VOG en geheimhoudingsverklaringen								
	Voert wanbeheer, slordigheden in beheersactiviteiten,								
	Werkt niet conform ITIL of BiSL principes								
	Maakt misbruik van toevertrouwde gegevens, applicaties en documentatie								
	Houdt zich niet aan functiescheiding								
	Maakt gebruik van te zware autorisatie, niet functiegebonden								