Model
Classificatie en Risicoanalyse Gegevensverwerkingen

GGZ Nederland, april 2016

Met dank aan Tactus verslavingszorg

Inhoud

Model classificatie en Risicoanalyse Gegevensverwerkingen

Op basis van wetgeving en beleid worden er hoge eisen gesteld aan het verwerken en opslaan van gegevens. Daarom dienen de gegevens binnen <*naam instelling*> geclassificeerd te worden op basis van hun integriteit, vertrouwelijkheid en beschikbaarheid.

Classificeren is een hulpmiddel om de beveiliging van gegevens binnen <*naam instelling*> vorm te geven en daarvoor is het noodzakelijk dat er een classificatieschema wordt gehanteerd. Classificatie van bedrijfsprocessen, informatiesystemen en informatie levert een bijdrage aan informatiebeveiliging.

Op basis van de classificatie van de gegevens kunnen prioriteiten voor beveiliging worden gesteld, 'beveiliging op maat' dus. Daarom wordt binnen <*naam instelling*> gebruik gemaakt van een classificatiesysteem om de verschillende beveiligingsniveaus te definiëren en per klasse specifieke minimumregels te stellen voor de beveiliging van bedrijfsprocessen, informatiesystemen en informatie.

Doelstelling
Dit model heeft tot doel de leden te helpen in hun wijze van classificeren van bedrijfsprocessen, informatiesystemen en informatie en deze te beschrijven. Hiermee worden de verantwoordelijken ondersteund om deze activiteit juist en volledig uit te voeren.

Risicoanalyse
De juiste klasse van beschikbaarheid, integriteit en vertrouwelijkheid voor het object van analyse wordt bepaald door het uitvoeren van een risicoanalyse. Deze activiteit wordt verricht door of namens de verantwoordelijke van het bedrijfsproces, informatiesysteem of de informatie.

Optioneel: De methode voor het uitvoeren van de risicoanalyse is vastgelegd in het < *naam moederdocument*> van <*naam instelling*>.

Indeling beschikbaarheid
Hoe kwalijk is het als de desbetreffende gegevens niet op korte termijn beschikbaar zijn of kunnen worden gemaakt?

	Beschikbaarheid	
Klasse	**Definitie**	**Voorbeeld**
Laag	Uitval van het bedrijfsproces, informatie(systeem) levert ***geen schade*** op voor <*naam instelling*>. Het is ook niet erg als de gegevens niet meer boven water komen	Voorlichtingsactiviteiten
Midden	Uitval van het bedrijfsproces, informatie(systeem) levert ***beperkte schade*** op voor <*naam instelling*>. Het proces/systeem mag een paar dagen niet beschikbaar zijn voordat er schade optreedt.	Scanproces
Hoog	Uitval van het bedrijfsproces, informatie(systeem) levert ***grote schade*** op voor <*naam instelling*>. De gegevens moeten altijd vrijwel onmiddellijk beschikbaar zijn, anders treedt er schade op	User

Indeling integriteit
Hoe kwalijk is het als gegevens ongemerkt worden veranderd gedurende de verzending/bewerking?

	Integriteit	
Klasse	**Definitie**	**Voorbeeld**
Laag	Onjuistheid of onvolledigheid van de uitvoering van het bedrijfsproces, van het informatie(systeem) levert geen schade op voor <*naam instelling*>. Geen enkel gevolg voor de bedrijfsvoering.	Agenda auditprogramma

Midden	Onjuistheid of onvolledigheid van de uitvoering van het bedrijfsproces, van het informatie(systeem) levert beperkte schade op voor <*naam instelling*>. Storend maar een oplosbaar probleem.	Verslag werkoverleg
Hoog	Onjuistheid of onvolledigheid van de uitvoering van het bedrijfsproces, van het informatie(systeem) levert grote schade op voor <*naam instelling*>. Forse schade, kan leiden tot bv faillissement, rechtszaak.	Elektronisch Dossier

Indeling vertrouwelijkheid

Hoe kwalijk is het dat betreffende gegevens bij de verkeerde ontvanger komen of publiekelijk verspreid worden? Voor de vertrouwelijkheid van bedrijfsprocessen, informatiesystemen en informatie wordt de volgende indeling in klassen gehanteerd.

	Vertrouwelijkheid	
Klasse	**Definitie**	**Voorbeeld**
Laag	Ongewenste openbaarmaking of verspreiding van de inhoud van het bedrijfsproces, van het informatie(systeem) levert geen schade op voor <*naam instelling*>. Geen enkel gevolg voor de bedrijfsvoering **= 'Openbaar'**	Cliëntenbrochure
Midden	Ongewenste openbaarmaking of verspreiding van de inhoud van het bedrijfsproces, van het informatie(systeem) levert beperkte schade op voor <*naam instelling*>. Storend maar wel een oplosbaar probleem > **= 'Voor intern gebruik'**	Projectadministratie

Hoog	Ongewenste openbaarmaking of verspreiding van de inhoud van het bedrijfsproces, van het informatie(systeem) levert grote schade op voor <*naam instelling*>. Forse schade, kan leiden tot bv faillissement, rechtszaak. **= 'Vertrouwelijk'**	Cliëntgegevens

Verantwoordelijkheden

De verantwoordelijkheden voor het classificeren van bedrijfsprocessen, informatiesystemen en informatie zijn als volgt verdeeld:

Verantwoordelijke bedrijfsproces/ Informatie(systeem)	bepalen van de classificatie o.b.v. risicoanalyse
Lijnmanagement	toezien op de naleving van <*het model*> voor classificatie en de hieruit voortvloeiende gebruiksregels
Security Officer	bijdrage leveren aan het bepalen van de classificatie; bepalen van de methode van classificatie en risicoanalyse
Audit	onafhankelijke controle naleving model classificatie

Controle en rapportage

Het lijnmanagement is verantwoordelijk voor de controle op de naleving van het beleid voor de classificatie van bedrijfsprocessen, informatiesystemen en informatie.

Onafhankelijke controle op de naleving van <*het model*> voor de classificatie van bedrijfsprocessen, informatiesystemen en informatie valt onder de verantwoordelijkheid van het auditteam. Deze controleactiviteiten worden uitgevoerd eventueel in overleg en in samenwerking met de externe accountant uitgevoerd. Hierover wordt gerapporteerd aan alle bij de controle betrokken functionarissen en instanties.

Procedures en overige verwijzingen

Bij <*dit model*> hoort het document …..