

CLA-R-1 Classificatie van bedrijfsprocessen, informatiesystemen en informatie

Inleiding

Classificatie van bedrijfsprocessen, informatiesystemen en informatie levert een bijdrage aan de beveiliging van deze bedrijfsprocessen, informatiesystemen en informatie. Op basis van de classificatie van deze objecten kunnen prioriteiten voor beveiliging worden gesteld, 'beveiliging op maat' dus. Daarom wordt binnen het Erasmus MC 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.

Hoofdpijn

Toelichting activiteiten

Het classificeren van bedrijfsprocessen, informatiesystemen en informatie omvat de volgende activiteiten:

- het kiezen van het object van analyse en classificatie; dit kan variëren van een bedrijfsproces, een informatiesysteem tot informatie (database, document, gegevensverzameling)
- het bepalen van de juiste klasse van beschikbaarheid, integriteit en vertrouwelijkheid voor het object van analyse door het uitvoeren van een risicoanalyse
- het vastleggen en bekend maken van de classificatie van het object van analyse aan alle betrokkenen
- het toepassen van de regels voor de beveiliging bij de uitvoering van het bedrijfsproces, c.q. het gebruik van het informatiesysteem of de informatie.

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. De methode voor het uitvoeren van de risicoanalyse is vastgelegd in het document 'Risicoanalysemethode Informatiebeveiliging Erasmus MC'.

Indeling beschikbaarheid

Voor de beschikbaarheid van bedrijfsprocessen, informatiesystemen en informatie wordt de volgende indeling in klassen gehanteerd.

	Beschikbaarheid	
Klasse	Definitie	Voorbeeld
Laag	Uitval van het bedrijfsproces, informatiesysteem en/of de informatie levert geen schade op voor het Erasmus MC	Voorlichtingsactiviteiten
Midden	Uitval van het bedrijfsproces, informatiesysteem en/of de informatie levert beperkte schade ¹ op voor het Erasmus MC	Financiële administratie
Hoog	Uitval van het bedrijfsproces, informatiesysteem en/of de informatie levert grote schade op voor het Erasmus MC	Patiëntenmonitoring

¹ Wat als 'beperkte' en 'grote' schade wordt aangemerkt, wordt door de verantwoordelijke op basis van de risicoanalyse bepaald.

Indeling integriteit

Voor de integriteit van bedrijfsprocessen, informatiesystemen en informatie wordt de volgende indeling in klassen gehanteerd.

	Integriteit	
Klasse	Definitie	Voorbeeld
Laag	Onjuistheid of onvolledigheid van de uitvoering van het bedrijfsproces, van het informatiesysteem en/of de informatie levert geen schade op voor het Erasmus MC	Menu personeelsrestaurant
Midden	Onjuistheid of onvolledigheid van de uitvoering van het bedrijfsproces, van het informatiesysteem en/of de informatie levert beperkte schade op voor het Erasmus MC	Verslag werkoverleg
Hoog	Onjuistheid of onvolledigheid van de uitvoering van het bedrijfsproces, van het informatiesysteem en/of de informatie levert grote schade op voor het Erasmus MC	Elektronisch patiëntendossier

Indeling vertrouwelijkheid

Voor de vertrouwelijkheid van bedrijfsprocessen, informatiesystemen en informatie wordt de volgende indeling in klassen gehanteerd.

	Vertrouwelijkheid	
Klasse	Definitie	Voorbeeld
Laag ‘Openbaar’	Ongewenste openbaarmaking of verspreiding van de inhoud van het bedrijfsproces, van het informatiesysteem en/of de informatie levert geen schade op voor het Erasmus MC	Patiëntenbrochure
Midden ‘Voor intern gebruik’	Ongewenste openbaarmaking of verspreiding van de inhoud van het bedrijfsproces, van het informatiesysteem en/of de informatie levert beperkte schade op voor het Erasmus MC	Intranet Erasmus MC
Hoog ‘Vertrouwelijk’	Ongewenste openbaarmaking of verspreiding van de inhoud van het bedrijfsproces, van het informatiesysteem en/of de informatie levert grote schade op voor het Erasmus MC	Informatie Experimenteel Dierencentrum

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 de richtlijn voor classificatie en de hieruit voortvloeiende gebruiksregels
- Coördinator Informatiebeveiliging bijdrage leveren aan het bepalen van de classificatie
- (Chief) Information Security Officer ((C)ISO) bijdrage leveren aan het bepalen van de classificatie
- bepalen van de methode van classificatie en risicoanalyse
- Audit onafhankelijke controle naleving richtlijn classificatie

Controle en rapportage

Het lijnmanagement (themavoorzitters, themadirecteuren, afdelingshoofden, directeuren, (sector)managers) is verantwoordelijk voor de controle op de naleving van de richtlijn voor de classificatie van bedrijfsprocessen, informatiesystemen en informatie.

Onafhankelijke controle op de naleving van de richtlijn voor de classificatie van bedrijfsprocessen, informatiesystemen en informatie valt onder de verantwoordelijkheid van de afdeling Audit. Deze controleactiviteiten worden eventueel in overleg en in samenwerking met externe auditors uitgevoerd. Hierover wordt gerapporteerd aan alle bij de controle betrokken functionarissen en instanties.

Documentatie

Bij deze richtlijn hoort het document 'Risicoanalysemethode Informatiebeveiliging Erasmus MC'.