

## BIV-classificatie Vf/Pf - **WEBAPPLICATIES**

De kwaliteitsaspecten die worden toegepast op informatiebeveiliging zijn Beschikbaarheid, Integriteit, en Vertrouwelijkheid. Deze termen worden hier inclusief de deelaspecten beschreven. Alle aspecten kunnen worden geclassificeerd in laag, midden en hoog.

### Beschikbaarheid:

Het waarborgen dat geautoriseerde gebruikers op de juiste momenten tijdig toegang hebben tot informatie en aanverwante bedrijfsmiddelen.

#### **Deelaspecten hiervan zijn:**

- Continuïteit: de mate waarin de beschikbaarheid van de ict-dienstverlening gewaarborgd is;
- Portabiliteit: de mate waarin de overdraagbaarheid van het informatiesysteem naar andere gelijksoortige technische infrastructuren gewaarborgd is;
- Herstelbaarheid: de mate waarin de informatievoorziening tijdig en volledig hersteld kan worden.

Voor de beschikbaarheid komt de classificatie *laag, midden en hoog* respectievelijk overeen met *niet nodig, belangrijk, noodzakelijk*.

### Integriteit:

Het waarborgen van de juistheid en de volledigheid van informatie en verwerking.

#### **Deelaspecten hiervan zijn:**

- Juistheid: de mate waarin overeenstemming van de presentatie van gegevens/informatie in IT-systemen ten opzichte van de werkelijkheid is gewaarborgd;
- Volledigheid: de mate van zekerheid dat de volledigheid van gegevens/informatie in het object gewaarborgd is;
- Waarborging: de mate waarin de correcte werking van de IT-processen is gewaarborgd.

Voor de integriteit komt de classificatie *laag, midden en hoog* respectievelijk overeen met *niet zeker, beschermd en hoog*

### Vertrouwelijkheid:

Het waarborgen dat informatie alleen toegankelijk is voor degenen die hiertoe is geautoriseerd.

#### **Deelaspecten hiervan zijn:**

- Autorisatie: de mate waarin de adequate inrichting van bevoegdheden gewaarborgd is;
- Authenticiteit: de mate waarin de adequate verificatie van geïdentificeerde personen of apparatuur gewaarborgd is;
- Identificatie: de mate waarin de mechanismen ter herkenning van personen of apparatuur gewaarborgd zijn;
- Periodieke controle op de bestaande bevoegdheden. Het (geautomatiseerd) vaststellen of geïdentificeerde personen of apparatuur de gewenste handelingen mogen uitvoeren.

Voor de vertrouwelijkheid komt de classificatie *laag, midden en hoog* respectievelijk overeen met *openbaar, bedrijfsvertrouwelijk en vertrouwelijk*

## Hoe bepaal ik het classificatie niveau?

Hiervoor maken we gebruik van de vragen, zoals deze zijn opgesteld voor het certificeringsschema. Praat over onderstaande vragen en maak een inschatting naar gewenst niveau. Het is misschien nog wel belangrijker om met een aantal mensen te praten over deze vragen, dan een exacte inschatting te maken. Door erover te praten kweek je bewustwording en ga je anders naar de processen kijken.

Beschikbaarheid				
<b>Uitleg</b> Bedenk welk <b>proces</b> de ICT-toepassing (in dit geval alle webapplicaties) ondersteunt. Vul aan de hand van onderstaande vragen een motivatie in en plaats een X in de bijbehorende kolom.				
Vragen	Motivatie	Laag	Midde n	Hoog
Wat is de verwachte belasting van de ict-toepassing? - Laag = weinig gelijktijdige gebruikers, weinig transacties (±1 per uur) - Midden = veel gelijktijdige gebruikers, normale hoeveelheid transacties (±10 per uur) - Hoog = veel gelijktijdige gebruikers, veel transacties (>100 per uur)	De webapplicaties zijn een breed scala aan producten, waardoor veel gelijktijdige gebruikers te verwachten zijn. Hierdoor <b>Hoog</b>			X
Wanneer moet de dienst beschikbaar zijn? - Laag = regulier (kantooruren) - Midden = ruim (bijvoorbeeld 07:00 - 23:00) - Hoog = altijd (24x7x365)	De webapplicaties zijn divers en voornamelijk gericht op schoolbesturen. Ook werkzoekenden is een doelgroep en deze is minder aan kantoor tijden gebonden, daardoor is <b>Midden</b> van toepassing.		X	
Zijn er contractuele of wettelijke verplichtingen voor de beschikbaarheid? - Laag = nee, of deze zijn regulier - Midden = er zijn contractuele verplichtingen en deze zijn ruim of hoog - Hoog = er zijn wettelijke verplichtingen	Nee, <b>Laag</b>	X		
Wat is de langste periode dat de ict-toepassing niet beschikbaar mag zijn? - Laag = maximaal enkele dagen - Midden = maximaal een werkdag - Hoog = maximaal een aantal uur	Gezien het gebruik en hoge beschikbaarheid mogen de webapplicaties maximaal een aantal uur niet beschikbaar zijn. <b>Hoog*</b>			X
Hoe erg is het als de data, informatie of de ict-toepassing niet beschikbaar zijn? - Laag = niet - Midden = het proces wordt belemmerd maar kan wel doorgaan - Hoog = het proces kan in zijn geheel niet doorgaan	Sommige processen kunnen niet doorgaan om dat bij processen er een afhankelijkheid is van de webapplicaties. <b>Hoog</b>			X
Leidt het niet beschikbaar zijn van de toepassing tot imagoverlies? - Laag = nee - Midden = kortstondig imagoverlies wat opgevangen kan worden door tijdige communicatie - Hoog = langdurig imagoverlies	De webapplicaties zijn het gezicht van VFPf en het directe contact met de klanten (buiten de adviseurs en coördinatoren). Het imago van VFPf is redelijk positief, maar komt van ver. Indien de webapplicaties het niet doen, is de verwachting dat het imagoverlies langdurig is, omdat het in het verleden ook niet altijd goed ging. Hierdoor <b>Midden</b> .		X	

- Buiten dienstverlenings window van 7-23u mag de beschikbaarheid langer onderbroken worden

<b>Niveau 1:</b> <b>Laag</b> Beschikbaarheid is onbelangrijk.	<b>Niveau 2:</b> <b>Midden</b> Beschikbaarheid is belangrijk	<b>Niveau 3:</b> <b>Hoog</b> Beschikbaarheid is noodzakelijk
De gegevens kunnen zonder gevolgen langere tijd niet beschikbaar zijn. Schending van beschikbaarheid heeft geen gevolgschade.	De informatie of service zou niet moeten uitvallen, het bedrijfsproces staat nauwelijks uitval toe. De continuïteit zal snel moeten worden hervat. Schending van deze classificatie kan serieuze (in)directe schade toebrengen.	De informatie of service zou niet moeten uitvallen, het bedrijfsproces staat nauwelijks uitval toe. De continuïteit zal snel moeten worden hervat. Schending van deze classificatie kan serieuze (in)directe schade toebrengen.

Integriteit				
<b>Uitleg</b> Bedenk welke <b>gegevens</b> de ict-toepassing (webapplicaties) ondersteunt. Vul aan de hand van onderstaande vragen een motivatie in en plaats een X in de bijbehorende kolom.				
Vragen	Motivatie	Laag	Midden	Hoog
Kan er fraude met leerresultaten of financiële fraude plaatsvinden door fouten in de gegevens of ongeautoriseerde wijzigingen? - Laag = nee, de gegevens lenen zich niet voor fraude - Midden = beperkt, gegevens worden ook elders gecontroleerd - Hoog = ja, de ict-toepassing is de enige toepassing met deze gegevens	De webapplicaties zelf bevatten geen gegevens, de gekoppelde applicaties wel. Hierdoor is dit voor de webapplicaties <b>Laag</b>	X		
Hoe erg is het als er fouten of ongeautoriseerde veranderingen in de gegevens zitten? - Laag = niet - Midden = het proces wordt belemmerd maar kan wel doorgaan - Hoog = het proces kan in zijn geheel niet doorgaan	De webapplicaties bevatten geen gegevens, muv tekstuele gegevens. Fouten hierin hebben een lage impact. <b>Laag</b>	X		
Hoeveel effect hebben fouten of ongeautoriseerde veranderingen in gegevens? - Laag = alleen intern - Midden = intern en bij een enkele ketenpartij - Hoog = in de hele keten	De webapplicaties bevatten geen gegevens, muv tekstuele gegevens. Fouten hierin hebben een lage impact. <b>Laag</b>	X		
Leiden fouten of ongeautoriseerde veranderingen tot imagoverlies? - Laag = nee - Midden = kortstondig imagoverlies - Hoog = langdurig imagoverlies	Indien teksten verkeerd staan kan dat verwaarloosbaar imagoverlies veroorzaken. <b>Laag</b>	X		
Zijn er contractuele of wettelijke verplichtingen voor de integriteit van gegevens? - Laag = nee - Midden = ja, deze eisen stelselmatige controle - Hoog = ja, deze eisen stelselmatige controle en bewijs van werking	Nee <b>Laag</b>	X		
Kunnen er personen negatieve gevolgen ondervinden als gevolg van het niet correct zijn van gegevens? - Laag = niet - Midden = eventuele fouten zijn nog te corrigeren - Hoog = fouten veroorzaken ernstige of langdurige negatieve gevolgen	Nee <b>Laag</b>	X		

<b>Niveau 1:</b> <b>Laag</b> Integriteit is onbelangrijk.	<b>Niveau 2:</b> <b>Midden</b> Integriteit is beschermd.	<b>Niveau 3:</b> <b>Hoog</b> Integriteit is noodzakelijk.
Deze informatie mag worden veranderd. Geen extra bescherming van integriteit is noodzakelijk. Schending van integriteit heeft geen gevolgschade.	Het bedrijfsproces dat gebruik maakt van deze informatie heeft geen directe hinder van (integriteits)fouten. Een basisniveau van beveiliging is noodzakelijk. Schending van deze classificatie kan enige (in)directe schade toebrengen.	Het bedrijfsproces dat gebruik maakt van deze informatie staat zeer weinig (integriteits)fouten toe. Bescherming van integriteit is absoluut noodzakelijk. Schending van deze classificatie kan serieuze (in)directe schade toebrengen.

<b>Vertrouwelijkheid</b>					
<b>Uitleg</b> <i>Bedenk welke gegevens de ict-toepassing (Webapplicaties) ondersteunt. Vul aan de hand van onderstaande vragen een motivatie in en plaats een X in de bijbehorende kolom.</i>					
<b>Vragen</b>	<b>Motivatie</b>	<b>Laag</b>	<b>Midden</b>	<b>Hoog</b>	
Wat is de classificatie van de gegevens? - Laag = publiek of intern gebruik - Midden = vertrouwelijk - Hoog = geheim	Een groot aantal webapplicaties heeft een inlogmechanisme. Hiermee krijgen gebruikers gegevens te zien die voor hem/haar van toepassing is. Deze gegevens zijn, in dit geval, vertrouwelijk en dus <b>Midden</b> .		X		
Worden personen waarvan gegevens lekken benadeeld door het lekken van gegevens? - Laag = nee - Midden = personen worden kortstondig benadeeld - Hoog = personen worden langdurig benadeeld	Het is aannemelijk dat indien gegevens lekken (bij ongeautoriseerde toegang), gezien de inhoud van de gegevens er sprake kan zijn van kortstondige tot langdurige nadelen. <b>Midden/Hoog</b>				X
Leiden datalekken tot imagooverlies? - Laag = nee - Midden = kortstondig imagooverlies wat opgevangen kan worden door tijdige communicatie - Hoog = langdurig imagooverlies	Indien ongeautoriseerd toegang verkregen wordt kan deze langdurig imagooverlies veroorzaken. <b>Hoog</b>				X
Zijn er contractuele of wettelijke verplichtingen voor de vertrouwelijkheid? - Laag = nee - Midden = ja, deze eisen bescherming - Hoog = ja, deze eisen bescherming, bewijs van werking en melding van inbreuk	Ja, BIR2017 en AVG regelgeving, <b>Hoog</b>				X
Welke type persoonsgegevens bevat de ict- toepassing? - Laag = geen - Midden = 'gewone' persoonsgegevens zoals NAW - Hoog = bijzondere persoonsgegevens (geloof, medisch, et cetera)	De toepassing zelf bevat geen persoonsgegevens, maar geeft wel toegang tot persoonsgegevens Geen <b>Laag</b>	X			
Kunnen er personen in gevaar worden gebracht als gevolg van het uitlekken van gegevens? - Laag = niet - Midden = eventuele fouten zijn nog te corrigeren - Hoog = personen kunnen het slachtoffer worden van identiteitsfraude	Met ongeautoriseerd toegang zijn criminelen in staat om identiteitsfraude te veroorzaken, <b>Hoog</b>				X

<b>Niveau 1:</b> <b>Laag</b> Informatie is voor openbaar gebruik	<b>Niveau 2:</b> <b>Midden</b> Informatie is vertrouwelijk.	<b>Niveau 3:</b> <b>Hoog</b> Informatie is geheim.
Alle informatie die algemeen toegankelijk is voor een ieder. Er is geen schending van deze classificatie mogelijk.	Informatie die toegankelijk mag of moet zijn voor alle medewerkers van de eigen organisatie. Vertrouwelijkheid is gering. Schending van deze classificatie kan enige (in)directe schade toebrengen.	Informatie die alleen toegankelijk mag zijn voor een beperkte groep gebruikers. De informatie wordt ter beschikking gesteld op basis van vertrouwen. Schending van deze classificatie kan serieuze (in)directe schade toebrengen.