Classificatiebeleid VfPf

Classificatie van data/informatie
Classificatie van systemen/applicaties

Vervangingsfonds
Participatiefonds

Versiebeheer

Versie	Datum	Wijziging	Auteur(s)
0.1		startdocument	Jolanda van Drunen, Avensus
0.99		Eerste bespreekversie	Mark Engels (strategisch adviseur informatiemanagement en architectuur)
0.993		Wijzigingen na eerste bespreking in team ISPMS	Ieke Coppens (PO/SO)
0.994		Verdere wijzigingen/aanvullingen	Ieke Coppens (PO/SO)
0.995		Verwerking review Matthieu Wieers (PO/SO) en verdere wijzigingen/aanvullingen	Ieke Coppens (PO/SO)
0.996		Verwerking review Mark Engels (strategisch adviseur informatiemanagement en architectuur)	Ieke Coppens (PO/SO)
0.997	29 november 2020	Wijzigingen/aanvullingen ter voorbereiding op bespreking 2/12/2020 in teams ISPMS	Ieke Coppens (PO/SO)
0.998	1 december 2020	Wijzigingen/aanvullingen nav finalisering P&S-beleid (synchronisatie)	Ieke Coppens (PO/SO)
0.999	4 december 2020	Wijzigingen/aanvullingen na bespreking in bespreking team ISPMS, finale check voorafgaand aan MT	Ieke Coppens (PO/SO)
1.0	14 januari 2021	Finale versie	Ieke Coppens (PO/SO)

Goedkeuring/vaststelling

Gremium	Datum	Besluit
MT	14 januari 2021	Instemming & vaststelling
Directie	14 januari 2021	Instemming & vaststelling

Distributielijst

Versie	Naam	Functie/doel
0.99	Matthieu Wieers, Jolanda van Drunen, Ieke Coppens	review
0.993	Matthieu Wieers, Mark Engels, Jolanda van Drunen	review
0.994	Matthieu Wieers, Mark Engels, Jolanda van Drunen	review
0.995	Matthieu Wieers, Mark Engels, Jolanda van Drunen	review
0.997	Matthieu Wieers, Mark Engels, Jolanda van Drunen	review
0.999	Directie en MT	Goedkeuring/vaststelling
1.0	Manager Bedrijfsvoering	Inbeheername

Inhoudsopgave

1. Inleiding

1.1. Classificatiebeleid in 8 begrippen[1]

Classificeren is het indelen in Classificaties. Classificaties zijn groepen van Data/Informatie en Systemen/Applicaties met gelijksoortige Betrouwbaarheidseisen. De Betrouwbaarheidseisen die VfPf stelt aan data/informatie en systemen/applicaties is per classificatie verschillend. De betrouwbaarheidseisen bepalen we aan de hand van een aantal criteria voor Beschikbaarheid, Integriteit en Vertrouwelijkheid. We korten deze betrouwbaarheidseisen af tot: BIV.

- *Beschikbaarheid: data/informatie en systemen/applicaties moeten op de juiste momenten **Beschikbaar** zijn: hebben gebruikers op de juiste momenten toegang tot de data/informatie en systemen/applicaties die ze voor hun werk nodig hebben?*
- *Integriteit: de data/informatie en systemen/applicaties moeten **Integer** zijn: is waar we mee werken en hoe we dat doen juist, is het volledig?*
- *Vertrouwelijkheid: de data/informatie en systemen/applicaties moeten **Vertrouwelijk** zijn en blijven waar dat nodig is: hebben alléén personen toegang tot data/informatie*

Hoe hoger de BIV-classificatie, hoe scherper de set maatregelen is die de Betrouwbaarheid ervan moet garanderen. Afhankelijk van periodieke analyses die we uitvoeren, herbeoordelen we de toegekende BIV-classificatie en de passendheid van de bijbehorende maatregelenset. Zo komen we blijvend tot "*passende technische en organisatorische maatregelen*".

Het Technisch beleid van VfPf beschrijft de basisset aan maatregelen die gelden voor de data/informatie in onze systemen/applicaties. Als de BIV-dataclassificatie van data/informatie in (de context van) onze systemen/applicaties een hogere BIV-score opleveren, stappen we over naar een scherpere set technische maatregelen. Zo kunnen we een hoger beschermingsniveau garanderen. Afhankelijk van specifieke risico's die we in risico-analyses zien, passen we de totale set technische en organisatorische maatregelen nóg verder aan. Hieronder volgen de kaders voor BIV-classificatie van systemen/applicaties.

1.2. Belang van classificatie

De betrouwbaarheid van alle data/informatie en van alle de systemen/applicaties waar deze data/informatie 'doorheen gaat', is van cruciaal belang voor onze strategische, tactische en operationele processen. Als de vaste maatregelenset niet "passend" is, is de betrouwbaarheid in de basis niet optimaal gegarandeerd. Daarmee loopt VfPf het risico dat niet wordt voldaan aan wettelijke eisen en regelgeving (niet compliant is). Het kan ertoe leiden dat VfPf boetes opgelegd krijgt van de Autoriteit Persoonsdata/informatie. Ook andere financiële schade kan het gevolg zijn. Denk ook aan reputatieschade en operationele beperkingen als systemen/applicaties of processen niet beschikbaar zijn.

Persoonsgegevens zijn een bijzondere vorm van data/informatie. Als er persoonsgegevens in het spel zijn staan ook de belangen op het spel van natuurlijke personen waarover die persoonsgegevens gaan: er

[1] Een lijst met de belangrijkste begrippen op het gebied van P&S tref je aan in de Begrippenlijst P&S. Voor de meest actuele versie van de P&S-begrippenlijst verwijzen we naar G:\Privacy en Security\1. P&S-beleid Vfpf, Infographic P&S VfPf en Handleiding AVG.

dreigen dan risico's van materiële en immateriële schade voor die betrokkenen. De Algemene verordening gegevensbescherming (AVG) legt VfPf daarom op om "passende technische en organisatorische maatregelen" te treffen om de Betrouwbaarheid van persoonsgegevens te waarborgen. (Dit geldt ook als de verwerking van persoonsgegevens is uitbesteed aan een leverancier. In de AVG wordt dit soort leveranciers Verwerkers genoemd.) De vertrouwelijkheid neemt hierbij een prominente plaats in, maar óók de Beschikbaarheid en Integriteit zijn bij persoonsgegevens van belang.

1.3. Reikwijdte/scope

In dit document leggen we het kader vast voor de classificatie van *data/informatie* en *systemen/applicaties*. De classificatie van *processen* wordt beschreven in het Bedrijfs Continuïteit Plan (afgekort tot BCP) van VfPf en zijn dus buiten scope van dit document.

1.4. Doelstelling

Het doel van dit document is het geven van een kader waarmee eenduidig wordt vastgesteld hoe we bij VfPf data/informatie en systemen/applicaties classificeren. In aanvulling op het Technisch beleid komen we zo tot "passende technische en organisatorische maatregelen", nu en in de toekomst. In dit document beschrijven we ook welke gevolgen de classificatie van data/informatie en systemen/applicaties heeft voor de technische maatregelen die we op de verschillende classificaties toepassen.

2. Kaders en uitgangspunten voor classificatie van data/informatie

2.1. Classificatie van data/informatie

Dataclassificatie begint bij het aanmaken van Informatiegroepen. Dat zijn soorten informatie die een bepaalde mate van vertrouwelijkheid gemeen hebben. Bij VfPf onderscheiden we er 4: openbare, interne, bedrijfsvertrouwelijke en vertrouwelijke informatie. Deze 4 Informatiegroepen zijn omschreven in onderstaande tabel. De blauwe kolom maakt in één oogopslag duidelijk hoe vertrouwelijk we die data/informatie vinden en aan wie we die data/informatie dus kunnen/mogen verstrekken.

Omschrijving Informatiegroep	**Wettelijke eisen**	**Classificatie Vertrouwelijkheid**	**Resultaat: Classificatie Informatiegroep**
Algemene informatie, publiekelijk beschikbaar, over activiteiten, producten en diensten van VfPf, zoals folders, leaflets, flyers, presentaties, rapportages en onderzoeken, bestuursbesluiten op de website VfPf, etc.	Geen	Openbaar: Informatie is publiekelijk beschikbaar en mag vrijelijk verstrekt worden	Classificatieniveau-0
Operationeel beleid, processen, procedures, plannen, rollen etc.	Geen	Intern gebruik: Informatie is beschikbaar voor alle interne medewerkers en door het management geselecteerde derde partijen. Deze informatie mag alleen aan interne medewerkers en door het management geselecteerde derde partijen verstrekt worden	Classificatiegroep-1
(Commercieel) vertrouwelijke stukken, zoals offertes, prijsopgaves, contracten, facturen en andere documenten met commercieel vertrouwelijke informatie. Verder bedrijfsinformatie over derde partijen (kengetallen, solvabiliteit e.d.) waarover VfPf beschikt, bv. in het kader van due diligence, etc. Verder ook de uitkomsten/rapportages over bv. pentesten in het kader van P&S	Wet toezicht financiële verslaglegging (Wtfv), Aanbestedingswet 2012	Bedrijfsvertrouwelijk: Informatie is alleen beschikbaar voor geautoriseerde personen. De informatie mag alleen aan geautoriseerde personen verstrekt worden, niet aan derde partijen	Classificatiegroep-2
(Persoons)gegevens van klanten, consumenten, werknemers en Bestuursleden, AC-leden etc., technische gegevens, configuraties, broncode, etc.	Algemene verordening gegevensbescherming (AVG) en Uitvoeringswet AVG (UAVG)	Vertrouwelijk: Informatie is alleen beschikbaar voor geautoriseerde personen. De informatie mag alleen aan geautoriseerde personen verstrekt worden, niet aan derde partijen	Classificatiegroep-3

2.2. Labeling

Labeling is het toevoegen van een (digitaal) ‘etiket’ aan documenten waaruit de gevoeligheid voor onbevoegde bekendmaking blijkt. Dit spitst zich dus toe op de Vertrouwelijkheid van de data/informatie in die documenten.

Bij VfPf worden documenten niet gelabeld. Uitgangspunt bij VfPf is dat documenten voor Intern gebruik zijn en dat deze niet met derden worden gedeeld.

3. Kaders en uitgangspunten voor BIV-classificatie van systemen/applicaties

3.1. Toekenning van BIV-classificaties van systemen/applicaties

Het vaststellen van de BIV-classificaties gebeurt aan de hand van de vragenlijsten die in de tabellen hieronder zijn opgenomen. Zo zijn er drie tabellen met vragen over Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV). Door alle vragen in de tabellen te beantwoorden en te motiveren ontstaat er een integraal en afgewogen beeld van de gewenste BIV-classificatie en dat maakt het makkelijk om de juiste Betrouwbaarheidseisen (BIV) operationeel te realiseren.

Deze tabellen met vragenlijsten zijn opgenomen in het template “BIV-classificering systemen/applicaties VfPf”. Alle vragen in het template moeten worden voorzien van de belangrijkste overwegingen van de risico-eigenaar om te komen tot de score per vraag: Laag, Midden of Hoog. De definities van die niveaus Laag, Midden en Hoog worden hieronder per betrouwbaarheidscriterium BIV gegeven. De hoogste score per BIV-vragenset bepaalt de einduitkomst van de BIV-classificatie.

3.2. Periodieke herbeoordeling BIV-classificaties van systemen/applicaties

Periodiek brengen we systematisch in beeld of de BIV-classificatie nog passend is. Ook beoordelen we periodiek aan welke dreigingen onze data/informatie en onze systemen/applicaties onderhevig zijn. Aan de hand van het Risico (= kans x impact) dat zo’n dreiging oplevert beoordelen we of de maatregelenset nog wel passend en effectief is. Zo niet, dan kan de maatregelenset worden bijgesteld.

Een belangrijk uitgangspunt is hierbij dat we risico’s prioriteren. Daarom brengen we in die risico’s een rangorde aan: Hoog, Midden of Laag. Uitgangspunten bij de omgang met deze risico’s zijn:

- *Als een risico als ‘laag’ wordt bestempeld dan kiezen we ervoor om dat risico te accepteren, tenzij het niet aanpakken van een laag risico op termijn tot een hoger risico kan leiden.*
- *Als een risico als ‘midden’ of ‘hoog’ wordt bestempeld neemt de risico-eigenaar in overleg met de directie altijd maatregelen, tenzij dat niet mogelijk is en/of de baten niet opwegen tegen de kosten.*

Deze periodieke herbeoordelingen van de BIV-classificatie van systemen/applicaties en de risico-analyses worden uitgevoerd door de risico-eigenaren en de directie, daarbij ondersteund door team P&S.

4. Vragenlijsten BIV-classificatie

4.1. Betrouwbaarheidscriteria voor Beschikbaarheid

Beschikbaarheid

Toelichting Denk bij het invullen ook aan het **proces** dat het system/applicatie ondersteunt. Vul aan de hand van onderstaande vragen een motivering in en plaats een X in één van de kolommen Laag, Midden of Hoog.

Vragen	Motivering	Laag	Midden	Hoog
Wat is de verwachte belasting van het system/applicatie? - 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)				
Wanneer moet de dienst beschikbaar zijn? - Laag = regulier (kantooruren, tussen 08:00 – 18:00 - Midden = ruim (bijvoorbeeld 07:00 - 23:00) - Hoog = altijd (24x7x365)				
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				
Wat is de langste periode dat het systeem/applicatie beschikbaar mag zijn? - Laag = maximaal enkele dagen - Midden = maximaal een werkdag - Hoog = maximaal een aantal uur				
Hoe erg is het als de data/informatie en/of de systemen/applicaties niet beschikbaar is/zijn? - Laag = niet - Midden = het proces wordt belemmerd maar kan wel doorgaan - Hoog = het proces kan in zijn geheel niet doorgaan				
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				

4.2. Betrouwbaarheidscriteria voor Integriteit

Integriteit

Uitleg Denk bij het invullen ook aan het **proces** dat het system/applicatie ondersteunt. Vul aan de hand van onderstaande vragen een motivering in en plaats een X in één van de kolommen Laag, Midden of Hoog.

Vragen	Motivering	Laag	Midden	Hoog
Kan er fraude plaatsvinden door fouten in de data/informatie of ongeautoriseerde wijzigingen? - Laag = nee, de data/informatie lenen zich niet voor fraude - Midden = beperkt, data/informatie worden ook elders gecontroleerd - Hoog = ja, de ict-toepassing is de enige toepassing met deze data/informatie				
Hoe erg is het als er fouten of ongeautoriseerde veranderingen in de data/informatie zitten? - Laag = niet - Midden = het proces wordt belemmerd maar kan wel doorgaan - Hoog = het proces kan in zijn geheel niet doorgaan				
Hoeveel effect hebben fouten of ongeautoriseerde veranderingen in data/informatie? - Laag = alleen intern - Midden = intern en bij een enkele ketenpartij - Hoog = in de hele keten				
Leiden fouten of ongeautoriseerde veranderingen tot imagoverlies? - Laag = nee - Midden = kortstondig imagoverlies - Hoog = langdurig imagoverlies				
Zijn er contractuele of wettelijke verplichtingen voor de integriteit van data/informatie? - Laag = nee - Midden = ja, deze eisen stelselmatige controle - Hoog = ja, deze eisen stelselmatige controle en bewijs van werking				
Kunnen er personen negatieve gevolgen ondervinden als gevolg van het niet correct zijn van data/informatie? - Laag = niet - Midden = eventuele fouten zijn nog te corrigeren - Hoog = fouten veroorzaken ernstige of langdurige negatieve gevolgen				

4.3. Betrouwbaarheidscriteria voor Vertrouwelijkheid

Vertrouwelijkheid

Toelichting Denk bij het invullen ook aan het **proces** dat het system/applicatie ondersteunt. Vul aan de hand van onderstaande vragen een motivering in en plaats een X in één van de kolommen Laag, Midden of Hoog.

Vragen	Motivering	Laag	Midden	Hoog
Wat is de classificatie van de data/informative die door het system/applicatie heengaan? - Laag = intern gebruik - Midden = vertrouwelijk - Hoog = bedrijfsvertrouwelijk of bedrijfsgevoelig				
Worden personen waarvan data/informatie lekken benadeeld door het lekken van data/informatie? - Laag = nee - Midden = personen worden kortstondig benadeeld - Hoog = personen worden langdurig benadeeld				
Leiden datalekken tot imagoverlies? - Laag = nee - Midden = kortstondig imagoverlies wat opgevangen kan worden door tijdige communicatie - Hoog = langdurig imagoverlies				
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				
Welke type persoonsdata/informatie bevat de ict-toepassing? - Laag = geen - Midden = 'gewone' persoonsdata/informatie zoals NAW - Hoog = bijzondere persoonsdata/informatie (geloof, medisch, et cetera)				
Kunnen er personen in gevaar worden gebracht als gevolg van het uitlekken van data/informatie? - Laag = niet - Midden = eventuele fouten zijn nog te corrigeren - Hoog = personen kunnen het slachtoffer worden van identiteitsfraude				