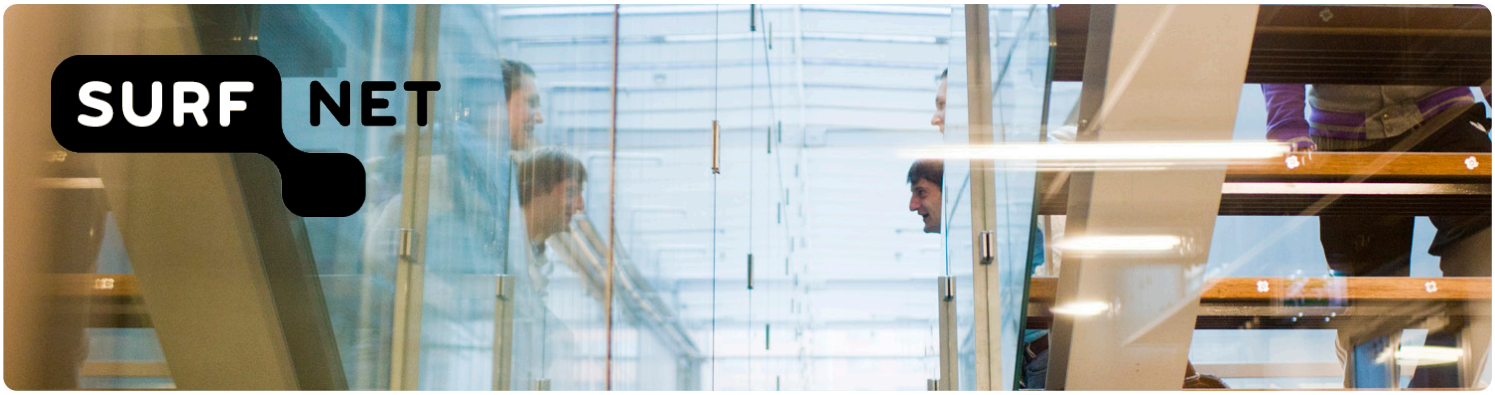


Leidraad classificatie

Toelichting en invulinstructie bij gebruik van het *classificatieformulier*

Auteur(s): Martin Romijn

Versie: 2.0

Datum: 18 november 2015

Moreelsepark 48
3511 EP Utrecht

Postbus 19035
3501 DA Utrecht

088 - 787 30 00
admin@surfnet.nl
www.surfnet.nl

ING Bank NL54INGB0005936709
KvK Utrecht 30090777
BTW NL 0089.60.173.B01

Colofon

SCIPR Leidraad Classificatie

SURF
PO Box 19035, 3501 DA Utrecht
T +31 88-7873000
info@surf.nl
www.surf.nl

Auteur
Martin Romijn

Kerngroep

Anita Polderdijk - Rijntjes	Windesheim
Bart van den Heuvel	Universiteit Maastricht
Menno Nonhevel	KNAW - Koninklijke Nederlandse Akademie van Wetenschappen
Alf Moens	SURFnet

Meelezers

Dubravka Marovic, Lilian Maas	Fontys	Corporate Information Security Officer
Edgar van Gorkum	Stenden	
Wim Koolhoven	Universiteit Twente	
Nick van der Laan	NWO	
Jean Popma	Radboud Universiteit	
Elma Middel	Hanzehogeschool	
Freerk Bosscha	Hogeschool NHL	
Peter Timmermans	Open Universiteit	
Hans van der Wal	Saxion	
Raoul Vernede	Wageningen Universiteit	
Haico Bianchi	Hogeschool Leiden	
Ronald Boontje	Universiteit van Amsterdam	Information Security Manager
Rene Ritzen	Universiteit Utrecht	Corporate Information Security Officer
Jelmar Boorsma	Vrije Universiteit	Information Security Officer

Eindredactie
Gezamenlijk product van de SCIPR en SURFnet

SURF is de ICT-samenwerkingsorganisatie van het hoger onderwijs en onderzoek (www.surf.nl).
Deze publicatie is digitaal beschikbaar via de website van SURFnet
(https://www.surf.nl/themas/digitale-rechten/privacy/index.html)

Inhoud

Woord vooraf / leeswijzer

In dit document stelt SCIPR (de SURF Community voor Informatiebeveiliging en Privacy) de leidraad classificatie voor. Deze voorgestelde leidraad beschrijft een *good practice* voor het classificeren van informatie. De leidraad bevat handvatten om een instellingseigen classificatierichtlijn te ontwikkelen of te verbeteren en deze te implementeren.
We bevelen aan de leidraad om te zetten in een interne classificatierichtlijn. Daarin kunnen de specifieke rollen en functionarissen zoals de instelling die noemt, worden gebruikt. De tekst in deze leidraad gaat namelijk uit van een *good practice* organisatiestructuur. Dat betekent concreet dat er wordt aangenomen dat er een CISO-rol is ingevuld (mogelijk onderdeel van een centraal CIO-office) en dat de eigenaren van processen benoemd zijn. Verder wordt aangenomen dat de FG-rol (Functionaris Gegevensbescherming) ingevuld is, of een Privacy Officer is aangesteld. Bij de omzetting naar een eigen richtlijn kan deze zodanig geformuleerd worden zodat deze past bij de eigen interne cultuur en governancestructuur.

In de leidraad is gekozen voor het classificeren van informatie in de context van het proces waarin deze informatie gebruikt wordt. De methodiek is tevens toepasbaar voor informatie in de context van een applicatie of systeem, door in de tekst “proces” te lezen als “applicatie” of “systeem”. Zowel in applicaties, systemen en processen wordt immers een set gegevensobjecten verwerkt. Met enige eigen interpretatie is deze leidraad dan inzetbaar voor het classificeren van een applicatie.

Uit het classificeren van een gegevensobject in meerdere contexten kan blijken dat de BIV-code per context verschilt. Een gegevensobject kan immers in verschillende processen, met verschillende eisen, voorkomen. Voorbeeld: de beschikbaarheidseis van een e-mailadres bij een acute roosterwijziging is hoog, een digitale nieuwsbrief kan gerust een dag later verstuurd worden.

Een aanvullend aspect dat voor zowel beschikbaarheid, integriteit en vertrouwelijkheid van belang is, is *controleerbaarheid*. Niet alleen “weten” of iets in orde is, maar dat ook achteraf kunnen “verifiëren”.

In Nederland zijn enkele methoden van classificeren in gebruik. In deze leidraad is gebruik gemaakt van een directe methode. Deze is eenvoudig toe te passen en voldoende adequaat. Vraag indien gewenst de collega CISO’s of SCIPR contactpersonen naar alternatieven.

Gebruikte termen

Term	Betekenis
Bedrijfsobject	Een bedrijfsobject is een passief element dat vanuit bedrijfsperspectief relevantie heeft [HORA]. De relevante bedrijfsobjecten in deze leidraad zijn gegevensobjecten. Voorbeelden van bedrijfsobjecten in de context van deze leidraad zijn alumnus, begroting en contact.
Beheerder	Een persoon die een systeem (al dan niet beroepsmatig) regelt en onderhoudt [Wikipedia]. In deze leidraad kan het beheren betrekking hebben op informatie, applicaties, databases en systemen in de rol van functioneel, technisch en/of applicatiebeheerder. Ook informatie kan een beheerder hebben.
BIA	Business Impact Analyse Een BIA wordt in het kader van het Business Continuity Management (BCM) gebruikt om de kritieke processen van de niet kritieke processen te scheiden [Wikipedia].

BIV-classificatie	Een BIV-classificatie of BIV-indeling is een indeling waarbij beschikbaarheid, (continuïteit), integriteit (betrouwbaarheid) en vertrouwelijkheid (exclusiviteit) van informatie en systemen wordt aangegeven [Wikipedia].
Beschikbaarheid	Informatie moet beschikbaar en toegankelijk zijn. Classificatie gaat in op de mogelijke gevolgen als informatie, of een informatieset, niet beschikbaar is.
Controleerbaarheid	De mate waarin het mogelijk is om achteraf parameters die van belang zijn voor beschikbaarheid, integriteit of vertrouwelijkheid te verifiëren. Zulke parameters zijn bijvoorbeeld downtime, toegang en transacties [Model beveiligingsbeleid uit het Framework Informatiebeveiliging Hoger Onderwijs, SCIPR, mei 2015].
Data	Data, ofwel gegevens, zijn objectieve feiten, teksten en getallen waaraan nog geen betekenis is gekoppeld.
Eigenaar	De afdeling/dienst/persoon of rol die over een zaak (stuk grond, voorwerp, hoeveelheid geld enz.) naar eigen goeddunken kan beschikken [naar Wikipedia]. In deze leidraad wordt met de eigenaar diegene bedoeld die het beslisrecht over een proces, applicatie, systeem, gegevenselement et cetera heeft. Wanneer de formeel eigenaar (vaak het College van Bestuur) het beschikkingsrecht overdraagt (mandateert) spreken we van functioneel of gedelegeerd eigenaar. Een eigenaar kan ook bestaan voor een organisatiebreed systeem en/of data in een organisatiebreed systeem.
Gegevens	Gegevens zijn de objectief waarneembare neerslag of registratie van feiten op een bepaald medium, zodanig dat deze gegevens uitgewisseld en voor langere tijd bewaard kunnen worden [Wikipedia]. Aan deze objectieve feiten is nog geen betekenis gekoppeld.
Informatie	Gegevens worden informatie als de gegevens een betekenis of nieuwswaarde hebben voor de ontvanger.
Integriteit	Het in overeenstemming zijn van informatie met de werkelijkheid (informatie is juist, volledig en actueel). Goed beheer van bevoegdheden en mogelijkheden tot muteren, toevoegen, of vernietigen van gegevens voor een gedefinieerde groep gerechtigden is cruciaal voor de integriteit van informatie. Classificatie gaat in op de mogelijke gevolgen wanneer informatie onjuist, onvolledig is of niet actueel is.
PIA	Een Privacy Impact Assessment (PIA) is een tool dat helpt bij het identificeren van privacy risico's en levert de handvaten om deze risico's te verkleinen tot een acceptabel niveau [Model Privacy Impact Assessment, werkgroep SURF-PIA].
Proces	Een bedrijfsproces is een ordening van het werk dat uitgevoerd dient te worden in een organisatie [Wikipedia].
Risicoanalyse	Een risicoanalyse is een methode waarbij nader benoemde risico's worden gekwantificeerd door het bepalen van de kans dat een dreiging zich voordoet en de gevolgen daarvan: Risico = Kans x Gevolg [Wikipedia].
Vertrouwelijkheid	De bevoegdheden en mogelijkheden om kennis te nemen van informatie voor een gedefinieerde groep gerechtigden. Classificatie gaat in op de mogelijke gevolgen wanneer informatie in handen komt van derden die hiertoe niet zijn geautoriseerd.

1. Inleiding

De Surf Community voor informatiebeveiliging en privacy (SCIPR), heeft op zich genomen de bestaande leidraad classificatie te moderniseren. Uitgangspunt voor de leidraad is dat instellingen veelal met dezelfde dreigingen te maken hebben, hetgeen ook blijkt uit het recente door SURF gepubliceerde rapport "Cyberdreigingsbeeld in het Hoger Onderwijs". Verder zijn de primaire processen binnen het Hoger Onderwijs in grote lijnen overeenkomstig.

Iedere instelling streeft naar een goede balans tussen het optimaal gebruik van ICT-middelen enerzijds en het borgen van de beschikbaarheid, integriteit en vertrouwelijkheid van informatie anderzijds. Deze doelstellingen bereiken we alleen met een gezamenlijke inspanning vanuit een functionele, technische en organisatorische invalshoek door beleid en uitvoering aangaande classificatie. Classificatie draagt bij aan:

- een veilige leer- en werkomgeving;
- een goed imago;
- naleving van wetgeving, zoals Wet bescherming persoonsgegevens (Wbp)[1].

Classificatie van informatie helpt bij:

- het selecteren van maatregelen die genomen moeten worden om informatie adequaat te beschermen, de integriteit te waarborgen en de beschikbaarheid te optimaliseren;
- het vergroten van de alertheid van de organisatie met betrekking tot de waarde van informatie en beveiligingsrisico's.

Informatie betekent in dit verband alle data en gegevens, ongeacht het medium waarop deze opgeslagen worden en ongeacht de presentatie daarvan. Informatie wordt in de praktijk verwerkt binnen één of meerdere bedrijfsprocessen en op één of meer systemen/applicaties. Deze context wordt dan ook bij de classificatie betrokken. Gekozen is voor het begrip "classificatie van informatie", in lijn met de naam van het vakgebied: "informatiebeveiliging".

1.1 Classificatie-aspecten: BIV

Het beschermingsniveau van informatie wordt uitgedrukt in classificatieniveaus voor Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV).

- Beschikbaarheid: informatie moet beschikbaar en toegankelijk zijn. Classificatie gaat in op de mogelijke gevolgen als informatie, of een informatieset, niet beschikbaar is.
- Integriteit: het in overeenstemming zijn van informatie met de werkelijkheid (informatie is juist, volledig en actueel). Goed beheer van bevoegdheden en mogelijkheden tot muteren, toevoegen, of vernietigen van gegevens voor een gedefinieerde groep gerechtigden is cruciaal voor de integriteit van informatie. Classificatie gaat in op de mogelijke gevolgen wanneer informatie onjuist, onvolledig is of niet actueel is.
- Vertrouwelijkheid: de bevoegdheden en mogelijkheden om kennis te nemen van informatie voor een gedefinieerde groep gerechtigden. Classificatie gaat in op de mogelijke gevolgen

[1] Vanuit de EU wordt naar verwachting in 2016 de Algemene Verordening Gegevensverwerking (AVG) van kracht. Tot de invoer van de AVG blijft de Wbp van kracht.

wanneer informatie in handen komt van derden die hiertoe niet zijn geautoriseerd.

1.2 Doelstelling classificatieproces: classificatie en maatregelen

Classificatie geeft een inschatting van de gevoeligheid en het belang van informatie om tot een juiste mate van beveiliging te komen. Niet alle informatie is even vertrouwelijk of hoeft bij een incident even snel weer beschikbaar te zijn. Het is niet erg efficiënt of gebruiksvriendelijk om niet-vertrouwelijke informatie op dezelfde manier te beschermen als vertrouwelijke informatie.

In dit document wordt een classificatieproces beschreven waarin niet alleen het feitelijke belang van informatie wordt bepaald in relatie tot de aspecten BIV, maar tevens de impact van eventuele inbreuken en de te kiezen risico beperkende maatregelen.

Informatieclassificatie hoort in elk project thuis waar informatie een rol speelt, maar zal ook op nieuwe toepassingen en bestaande omgevingen moeten worden uitgevoerd. Zo kan door veranderende processen de waarde van informatie in de loop van de tijd veranderen. Ook het niveau van dreiging kan veranderen. Daardoor kunnen de benodigde beschermingsmaatregelen veranderen.

1.3 Classificatie versus Risicoanalyse

Met een risicoanalyse kan de mogelijke schade worden geëvalueerd die een dreiging kan toebrengen aan specifieke informatie (bijv. misbruik door oneigenlijke toegang, ongeautoriseerde toegang) en wat de kans is dat die schade optreedt. Het management dient vervolgens aan te geven welke risico's aanvaardbaar zijn en welke met maatregelen moeten worden afgedekt.

Het gebruik van standaard risicoanalyse hulpmiddelen is vaak een tijdrovend en abstract traject. De in deze leidraad voorgestelde classificatiemethodiek geeft een goede indicatie van het belang van de informatie. Gekoppeld aan de classificatie worden maatregelen geselecteerd die de kans op en de impact van inbreuken op de veiligheid terugdringen tot een voor de organisatie acceptabel niveau. De classificatie kan gezien worden als een risicoanalyse op basis van algemene waarden in plaats van concrete risico's. Er kan dan ook altijd besloten worden alsnog een uitgebreide risicoanalyse uit te voeren.

1.4 Baseline informatiebeveiliging versus Classificatie en Maatregelen

De meeste instellingen hebben een baseline vastgesteld voor Informatiebeveiliging. SCIPR heeft daartoe een Baseline Informatiebeveiliging HO (BIHO) ontwikkeld. De BIHO beschrijft basismaatregelen die elke instelling altijd zou moeten implementeren. Dit zijn algemene maatregelen, zoals het vaststellen van IB-beleid, plus maatregelen die te relateren zijn aan de classificatieaspecten beschikbaarheid, integriteit en vertrouwelijkheid.

De maatregelen in de BIHO zijn generiek en hebben dan ook een relatief hoog abstractieniveau. Ten behoeve van informatieclassificatie is er een set operationele maatregelen benodigd, passend bij de niveaus Laag, Midden en Hoog voor beschikbaarheid, integriteit en vertrouwelijkheid. Het verdient aanbeveling een basisset operationele maatregelen specifiek voor de eigen instelling op te bouwen. De praktijk heeft uitgewezen dat de set organisatiespecifiek is en daardoor vooralsnog niet als operationele baseline vanuit SCIPR aangeboden kan worden. Ter inspiratie kan voortgebouwd worden op de voorbeeldmaatregelen die in het classificatieformulier zijn opgenomen.

Uit de BIV classificatie volgt welke operationele maatregelen geïmplementeerd moeten worden. In het classificatierapport wordt van al deze maatregelen aangegeven of en hoe deze geïmplementeerd zijn/worden conform het principe “pas toe of leg uit”.

NB: Aanbevolen wordt om voor de instelling een “default classificatieniveau” vast te stellen wat overeenkomt met de baseline en een balans vormt tussen maximale risico’s en minimale kosten.

Een good practice is B=Midden, I=Midden en V=Hoog (BIV=MMH). Hierdoor worden geen heel dure maatregelen genomen voor B en I, terwijl voor Vertrouwelijkheid (privacy) zo weinig mogelijk risico’s worden genomen. Onderliggende gedachte is dat op deze manier voldaan kan worden aan de nationale en Europese regelgeving als de Europese DPA, Wbp, wet Meldplicht Datalekken (vertrouwelijkheid) en de informatie-eigenaren uitgedaagd worden om een classificatie uit te voeren.

Trend is dat steeds meer data open beschikbaar wordt. Daar waar dat het geval is, wordt het vertrouwelijkheidsniveau van leermaterialen en onderzoekgegevens laag.

In bijlage IV is een voorstel voor classificatie voor een serie veel voorkomende gegevensobjecten opgenomen. Daar waar de HORA een classificatie voorgesteld heeft is deze overgenomen, de ontbrekende zijn in het kader van deze leidraad door de kerngroep toegevoegd.

1.5 Bronnen

De volgende bronnen zijn gebruikt:

Referentienaam	**Versie**	**Auteur**
Model beveiligingsbeleid uit het Framework Informatiebeveiliging Hoger Onderwijs	2.0	SURFibo
Hoger Onderwijs Referentie Architectuur (HORA)		Werkgroep Architectuur
SurfIBO leidraad classificatie definitief, juli 2010	1.0	SURFibo
Fontys Werkwijze Classificatie en risico-analyse	1.2	Lilian Maas
Template Classificatiesysteem Windesheim	2.0	Anita Polderdijk-Rijntjes
Classificatie-richtlijnen-UM	1.2	Bart van den Heuvel
Wikipedia, verschillende definities	10-2015	Gemeenschap
Richtsnoer “Beveiliging van persoonsgegevens”	02-2013	CBP

2 Classificeren van informatie

Dit hoofdstuk beschrijft uitgangspunten, verantwoordelijkheden, niveaus

2.1 Uitgangspunten

- Alle gegevens, applicaties, processen en systemen hebben een eigenaar.
- De (gemandateerd) eigenaar bepaalt de classificatie (het vereiste beschermingsniveau) en welke restrisico's aanvaardbaar zijn.
- De CISO, in afstemming met gebruikersorganisatie en ICT, bepaalt wat bij het beschermingsniveau passende beveiligingsmaatregelen zijn.
- Bij de verwerking van informatie kan het classificatieniveau van het proces/systeem waarin bepaalde informatie gebruikt wordt anders uitvallen dan puur op basis van de classificatie van de informatie verwacht zou worden.
- Er wordt gestreefd naar een verantwoord, maar zo 'laag' mogelijk classificatieniveau; overbodig hoge classificatie leidt tot onnodige drempels en kosten.
- De CISO beheert het register van alle classificatierapporten en initieert de periodieke review door de eigenaar.

2.2 Verantwoordelijkheden en Werkwijze Classificatie

De eigenaar heeft de eindverantwoordelijkheid voor de uitvoering en het resultaat van de classificatie. De eigenaar beslist over (wijzigingen in) functionaliteit, voert op basis daarvan de informatieclassificatie uit en draagt de kosten die verband houden met informatiebeveiliging. De eigenaar is verantwoordelijk voor de implementatie en opvolging van de afgesproken beveiligingsmaatregelen.

Het CIO Office/ de CISO is verantwoordelijk voor beleid, kaders en richtlijnen op het gebied van informatiemanagement en informatiebeveiliging, bepaalt de methode van de informatieclassificatie en risicoanalyse en levert een bijdrage aan het bepalen van de informatieclassificatie in overleg met de functioneel eigenaren van de informatie en/of IT-voorziening.

De classificatie zal in groepsverband worden uitgevoerd met een aantal betrokkenen, minimaal de eigenaar, CISO en een functioneel beheerder. Dit zorgt voor een lerend effect, geeft commitment binnen de groep, zorgt voor samenwerken en vooral voor een goed gewogen gemiddelde.

De CISO stelt vervolgens maatregelen voor in overleg met betrokkenen (in ieder geval functioneel beheer, soms ook de (interne/externe) ICT-leverancier in verband met de technische mogelijkheden.

De BIV-scores, de ingevulde vragenlijsten, een samenvatting, de afspraken over te nemen maatregelen en een eventueel vastgesteld restrisico worden door de CISO verwerkt in een classificatierapport dat uiteindelijk door de eigenaar formeel wordt vastgesteld.
In het kader van reproduceerbaarheid en voor bijvoorbeeld audits of om vergelijkingen te kunnen maken bij toekomstige her-classificaties, worden deze classificatierapporten gearchiveerd door de CISO.

2.3 Classificatie-niveaus

De onderscheiden niveaus voor de aspecten B,I en V zijn verdeeld in drie categorieën: laag, midden, hoog. Onderstaande tabel geeft een indicatie van de betekenis van deze categorieën.

categorie	schade	beschikbaarheid[2]	integriteit	vertrouwelijkheid
laag	Inbreuk op beveiliging bij deze classificatie kan enige (in)directe schade toebrengen.	algeheel verlies of niet beschikbaar zijn van deze informatie gedurende langer dan 1 week brengt geen merkbare (meetbare) schade toe aan de belangen van de instelling, haar medewerkers of haar studenten of klanten	het bedrijfsproces staat enkele integriteitsfouten toe.	informatie die toegankelijk mag of moet zijn voor alle of grote groepen medewerkers of studenten. Vertrouwelijkheid is gering. Daar waar informatie openbaar is, is inzage geen issue, beheer (ten behoeve van de integriteit) wel.
midden	Inbreuk op beveiliging bij deze classificatie kan serieuze schade toebrengen.	algeheel verlies of niet beschikbaar zijn van deze informatie gedurende langer dan 1 dag brengt merkbare schade toe aan de belangen van de instelling, haar medewerkers of haar studenten of klanten	het bedrijfsproces staat zeer weinig integriteitsfouten toe. Bescherming van integriteit is absoluut noodzakelijk.	informatie die alleen toegankelijk mag zijn voor een beperkte groep gebruikers. De informatie is vertrouwelijk.
hoog	Inbreuk op beveiliging bij deze classificatie kan zeer grote schade toebrengen.	algeheel verlies of niet beschikbaar zijn van deze informatie gedurende langer dan 1 uur brengt merkbare schade toe aan de belangen van de instelling, haar medewerkers of haar studenten of klanten	het bedrijfsproces staat geen integriteitsfouten toe.	dit betreft zeer vertrouwelijke informatie, alleen bedoeld voor specifiek benoemde personen, waarbij onbedoeld bekend worden buiten deze groep grote schade kan toe brengen.

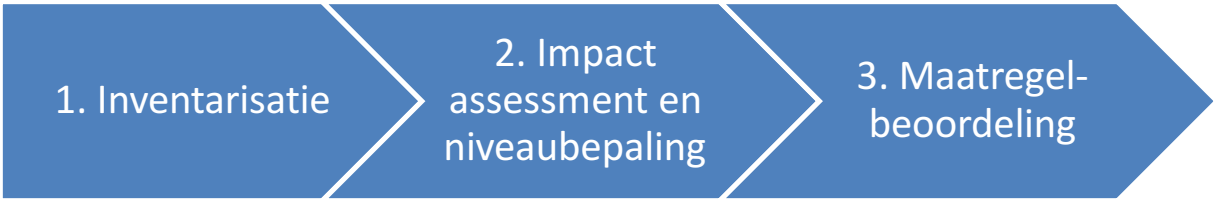
[2] Definities uit het Model informatiebeveiliging SCIPR (voorheen SURFibo)

3 Het classificatieproces

Het proces van classificatie verloopt in interactie tussen de eigenaar van de informatie en de CISO. De eigenaar deelt diens inschatting van het belang en de bedrijfsrisico's met de CISO, waarna gezamenlijk conclusies worden getrokken en passende maatregelen worden geselecteerd. De classificatie maakt in veel gevallen een tijdrovende en abstracte risicoanalyse overbodig.

3.1 De fasen in het classificatieproces

De drie hoofdfasen van de classificatie zijn als volgt:



1. I**nventarisatie**
   De informatieclassificatie start met vaststellen om welke gegevensobjecten het gaat, welk bedrijfsproces(sen), informatiesysteem en welke wet- en regelgeving mogelijke eisen stelt aan het gebruik, distributie en opslag. Denk bijvoorbeeld aan bewaartermijnen en de Wet bescherming persoonsgegevens (Wbp). Van de informatie-elementen wordt een eerste classificatie van de BIV aspecten vastgesteld. De vragenlijst Inventarisatie is hiervoor bedoeld. Deze vragenlijst is bij deze leidraad opgenomen in het eerste tabblad van het separate Excel bestand. Van het Excel bestand kunnen de vragen indien gewenst overgezet worden naar Word of een tool voor beheer van vragenlijsten.
2. **Impact assessment en niveaubepaling**
   Aansluitend op de inventarisatie wordt bepaald hoe groot de kans op en de impact van inbreuken is op de BIV aspecten. Deze inschatting leidt tot de eindclassificatie voor beschikbaarheid, integriteit en vertrouwelijkheid. Deze eindklasse is richtinggevend voor de bijpassende maatregelen. De maatregelen zijn door de instelling vooraf in een de operationele maatregelenset opgenomen. Een voorbeeldset met maatregelen is in het classificatieformulier opgenomen. Het classificatieformulier is daardoor bedoeld voor de impact- en niveaubepaling plus eerste selectie van maatregelen.
3. **Beoordelen maatregelen**
   In deze stap wordt gekeken of de hiervoor vastgestelde maatregelen volstaan, deze reeds zijn geïmplementeerd, of dat er aanvullende acties nodig zijn c.q. of bepaalde restrisico's acceptabel zijn. Het model classificatierapport is bedoeld voor de beoordelingsfase.

Vertaald naar stappen in het proces zijn dit:

1. De eigenaar of gedelegeerd (functioneel) beheerder vult vragenlijsten in
2. De CISO bestudeert de vragenlijsten en vormt zich een mening
3. Eigenaar en CISO bespreken de vragenlijsten en bepalen de eindscore van de BIV-classificatie
4. De te treffen maatregelen worden overgenomen uit de operationele BIV-maatregelenset.
5. Eigenaar en CISO gaan na of de overgenomen maatregelen volstaan, waar afwijkingen mogelijk of noodzakelijk zijn en welke restrisico's acceptabel zijn.
6. CISO stelt een classificatierapport met eindadvies op dat door eigenaar wordt vastgesteld.

De afstemming tussen eigenaar en CISO zal soms gaan over de juistheid van het geconcludeerde niveau. Moet de beschikbaarheid daadwerkelijk zo hoog zijn? Is het verzamelen van deze informatie daadwerkelijk nodig, of kan volstaan worden met minder vertrouwelijke gegevens- of verzamelingsvorm? Soms gaat het over kosten, de noodzaak van maatregelen en mogelijke alternatieven. Aanvullende maatregelen met betrekking tot beschikbaarheid kunnen misschien ook in het te ondersteunen proces genomen worden, waardoor uitval van een systeem minder impact heeft. Aanvullende maatregelen zoals encryptie of anonimiseren kunnen het risico met betrekking tot vertrouwelijke informatie beperken. In zulke gevallen kunnen minder zware maatregelen op systeemniveau mogelijk voldoende zijn. In het uiteindelijke advies komen alle overwegingen en conclusies samen.

3.2 Kerneigenschappen per processtap

De onderstaande tabel zet de processtappen achter elkaar en geeft per processtap de belangrijkste kenmerken weer.

Kenmerk	Scope leidraad classificatie			Buiten scope	
STAP	**1. Inventarisatie**	**2. Impact en niveau bepaling**	**3. Maatregel beoordeling**	**Risicoanalyse**	**PIA**
SETTING	Eigenaar of functioneel beheerder	Eigenaar en CISO	CISO met eigenaar	Eigenaar, beheerder, key users	Verantwoordelijke met FG, security en/of privacy officer
WERKWIJZE	Invullen vragenlijsten	Gesprek over het assessment	Workshop over standaard maatregelen	Desk research en workshop(s)	Verzamelen informatie, inschatten risico's en
TOOLS	Vragenlijsten	Classificatie formulier	Samenvatting classificatie-rapport	Extern (Internet)	Model PIA SURF/SCIPR
RESULTAAT	Basisinzicht in eisen en context	Eindclassificatie BIV bepaald	Maatregelen passend bij BIV-niveau	Gedetailleerd inzicht in risico's en maatregelen	Gedetailleerd inzicht in risico's en maatregelen
UREN INDICATIEF	2 uur per invuller	2 uur CISO, 1 uur per overige deelnemer	1,5 uur per deelnemer	16 uur	8 uur

Schema met kenmerken per processtap geïnspireerd op de presentatie van de IBD bij VNG dd 6 oktober 2014

Toelichting bij buiten scope:
Als de classificatie van de beschikbaarheid, integriteit of vertrouwelijkheid op Hoog uit komt en het

assessment niet leidt tot vertrouwen in de juistheid van de gekozen set maatregelen, wordt het uitvoeren van een risicoanalyse geadviseerd.

Als uit het invullen van de inventariserende vragenlijst blijkt dat persoonsgegevens verwerkt worden, dan is [volgens richtsnoer het CBP] een risico analyse verplicht en daarvoor is een PIA het aanbevolen instrument. Artikel 13 van de Wbp vereist bij de beveiliging van persoonsgegeven een risicogerichte benadering[3]. De PIA kan aanleiding geven tot een hoge(re) classificatie op het aspect vertrouwelijkheid en eventueel ook tot aanvullende specifieke maatregelen, zeker als één of meer van de volgende situaties gelden:

- gegevens betreffen kwetsbare groepen in de samenleving (bejaarden, kinderen, patiënten,..);
- gegevens betreffen grote groepen personen;
- de veiligheid van betrokken loopt (ernstig) gevaar als persoonsgegevens uitlekken of onterecht worden verwerkt;
- uitlekken van de persoonsgegevens kan tot identiteitsfraude leiden met grote persoonlijke of organisatorische schade tot gevolg (financieel, imago);
- uitlekken of onterecht verwerken kan bij betrokkenen ernstige fysieke en/of geestelijke schade veroorzaken.

Soms is het wenselijk in vroeg stadium van een business case of projectinitiatie een eerst, globaal beeld van de informatie-elementen en context te verkrijgen. In die situatie kan de inventariserende vragenlijst ingezet worden.

[3] Pagina 17 CBP richtsnoer “Beveiliging van persoonsgegevens”, februari 2013.

Bijlage I: Schadecategorieën

Soms is bij het bespreken van de vragenlijsten het bepalen van de impact onderbuikgevoel. Onderstaande tabel poogt enige objectiviteit in te brengen. De gevolgschadetabel probeert vervolgens aan te geven worden hoe sterk op maatregelen ingezet moet worden. De aanduidingen zijn indicatief en ook de frequentie waarmee gebeurtenissen plaatsvinden spelen een rol.

	Schadecategorieën			
Gevolg schade	**financieel**	**imago**	**onderwijs**	**certificatie**
klein	Directe schade ligt tussen 0 en €50.000	Een klein aantal negatieve berichten in lokale media (inclusief sociale media)	Hooguit verstoring van een beperkt aantal activiteiten op een instituut of vakgroep.	Geen invloed op onderwijscertificatie
middel	Directe schade tussen €50.000 en €250.000	Negatieve berichtgeving in de media gedurende een paar dagen (inclusief sociale media)	Verstoring van een deel van het onderwijs (zoals een deel van instituut of vakgroep)	Extra toezicht op onderwijscertificatie
groot	Directe schade tussen €250.000 en €1.500.000	Aanhoudende negatieve berichtgeving in de lokale media (inclusief sociale media)	Verstoring van een groot deel van het onderwijs op een of meer instituten.	Beperking van onderwijscertificatie
catastrofaal	Directe schade is groter dan €1.500.000	Aanhoudende negatieve berichtgeving in de landelijke media (inclusief sociale media)	Merendeel van het onderwijs wordt onmogelijk op een of meer instituten	Verlies van onderwijscertificatie

Gevolgschade	**B, I of V classificatie**
Klein	L (laag)
Middel	M (midden)
Groot	M of H (hoog)
Catastrofaal	H grote hoeveelheden of continuïteit in gevaar

Risico	**Gevolgschade**			
Kans op inbreuk	klein	middel	groot	catastrofaal
dagelijks				
maandelijks				
jaarlijks				
zelden				

	Risico valt onder Business Continuity Management
	ontoelaatbaar risico
	bespreekbaar risico
	acceptabel risico

Bijlage II: Template Samenvatting classificatierapport

Algemeen			
Functioneel eigenaar	Dienst ..		
Functie			
Telefoonnummer			
Laatste datum invullen			
Te classificeren onderwerp			
Informatie	o.a. Studentgegevens, …[4]		
Risico's	<algemene beschrijving risico's>		
Classificatie en risicoanalyse			
	Beschikbaarheid	Integriteit	Vertrouwelijkheid
Geadviseerd beveiligingsniveau			
Eindadvies	X voldoet in de huidige constructie WEL / NIET aan het model van informatieclassificatie, indien voldaan wordt aan de onderstaande acties		
Acties	A. B. C.		

Is er een motivatie om af te wijken van de conclusie (door de functioneel eigenaar)? Ja / Nee

Indien er een afwijking is:

- Geef de afwijking, eventueel tegenmaatregel en het restrisico aan
- Is het restrisico acceptabel? Ja / Nee

Aldus opgemaakt d.d.: Naam functioneel eigenaar:

[4] Bij voorkeur wordt in het volledige rapport een compleet overzicht geleverd van alle gegevens- en bedrijfsobjecten

Bijlage III: Voorbeeld vragenlijst "Inventariserend"

Eigenaarschap	
Naam verantwoordelijke dienst/opleiding	Dienst Onderwijsondersteuning
Naam hoofd/leidinggevende	Jolanda Peters
Functie	Directeur Onderwijsondersteuning
Contactgegevens	j.peters@instelling.nl
Invuldatum	1 oktober 2015
Inleiding	
Naamsaanduiding proces Naam en korte omschrijving van het proces	Beheren studieresultaten
Functionele doelen Wat dient met het proces bereikt te worden; welke deelprocessen bevat het proces?	▪ Bewaken studievoortgang ▪ Coaching studenten ▪ Diplomeren/Certificeren
Typen werkplekken Waar worden de werkzaamheden in dit proces uitgevoerd? Met andere woorden: voor welke typen werkplekken is raadpleging en/of mutatie van gegevens bedoeld? Vermeld hier de mogelijkheden voor kantoor, thuis via internet en mobiel	▪ Kantoor (door instelling beheerde werkplek) ▪ Onderweg (BOYD en instellingslaptop) ▪ Thuis (privé PC, laptop)
Ketenverbindingen Worden in dit proces gegevens verzameld die hergebruikt worden in andere processen, en om welke gegevens gaat het dan? Vermeld indien relevant ook de ontvangende systeem- of toepassingsnamen en de naam van de eigenaar/eigenaren daarvan.	▪ Studentgegevens vanuit inschrijfproces ▪ Studenten en groepen naar ELO ▪ Afgestudeerden naar examenregister en CRM ▪ Contactgegevens naar SMS server
Aanduiding gegevens	
Welke gegevenstypen worden vastgelegd? Denk aan teksten, tabellen, plaatjes e.d.	Gestructureerde gegevens als contactgegevens, teksten (verslagen, rapporten, werkstukken), studieresultaten (beoordelingen).

Welke gegevenselementen worden vastgelegd?

Denk aan meetresultaten, personalia, locaties, financiën e.d. Benoem nadrukkelijk gegevens die concurrentie- of fraudegevoelig zijn, en informatie die direct of indirect herleidbaar is naar natuurlijke personen.

Gegevenselement HORA	BIV-code
Opleiding	MHL
Minor	MHL
Onderwijsprogramma	MHL
Onderwijseenheiduitvoering	MHL
Onderwijseenheiddeelname	MML
Examenprogramma	MHL
Toetsresultaat	LHM
Onderwijseenheidresultaat	LHM
Onderwijsovereenkomst	LML
Deelnemer	MHH
Waardedocument	LHL
Lesgroep	MML
Leergroep	LML
Competentie	LLL
Onderwijsactiviteit	MML
Deelnemeractiviteit	MMH

Worden privacygevoelige gegevens vastgelegd?

Als gegevens opgeslagen of verwerkt welke herleidbaar zijn tot natuurlijke personen dan is een uitvoeren van een PIA verplicht.

Ja. Naar persoon te herleiden studieresultaten (deelcijfers en cijfers). Ook verslagen van studiebegeleiders en samenvatting van psychologische gesprekken en tests.

Mutatiebevoegdheden

Hoeveel personen krijgen rechten om de gegevens te muteren?
Maak hierbij onderscheid: autorisatie van gebruikers, mutatie van systeemtabellen, invoer van transacties e.d. Vermeld ook de rechten van (externe) consultants bij uitbreiding of onderhoud.

- Beheerders (6): onderhoud referentietabellen
- Back office (14): onderhouden opleidingsspecifieke informatie
- Cijfersadminstratie (3): invoeren/corrigeren resultaten voor toegewezen faculteiten
- Docenten (600): vastleggen resultaten
- Studiebegeleiders (6): gespreksverslagen, voorzieningen voor toegewezen studenten
- Studenten (6000): Eigen gegevens onderhouden

Raadpleegbevoegdheden

Hoeveel personen krijgen rechten om de gegevens in te zien?
Maak hierbij onderscheid: algemene raadpleegfuncties, persoonlijke gegevens van alleen de gebruiker zelf e.d.

- Back office: volggegevens voor alle faculteiten
- Docenten/Studenten: eigen persoonlijke gegevens
- Studiebegeleiders: begeleidingsgegevens alle student

Bewaartermijnen

Hoe lang worden gegevens bewaard (nadat ze bedrijfsmatig zijn afgehandeld)? Denk hierbij aan afgegeven diploma's, promoties, pensioengegevens enzovoorts. Specificeer de termijnen, bijvoorbeeld na een jaarafsluiting of na diploma-uitreiking of pensionering.

Gegeven	Periode
Studenten eerste inschrijving	2 jaar na uitschrijving
Studenten inschrijving collegejaar	7 jaar na inschrijving
Numerus fixus	7 jaar na aanpassing
Buitenlandse studenten toelating	5 jaar na inschrijving
Studievoortgang bewaking	1 jaar na accountantscontrole
Studenten financiële ondersteuning	7 jaar na verstrekking
Studenten bijzondere voorziening	7 jaar na inschrijving
Studenten schorsing	10 jaar na ontzegging
Studenten weigering verwijdering	5 jaar na weigering of verwijdering
Studenten uitschrijving	5 jaar na uitschrijving

	Verklaring behaalde tentamens	1 jaar na uitgifte
Archivering Is het de bedoeling dat historische gegevens vastgelegd dan wel periodiek weggeschreven naar andere media? Bedoeld is hier een interne en/of externe archiveringsfunctie en de regelmaat waarmee dit gebeurt.	Bovenstaande gegevens met bewaartermijn “Bewaren” worden 1 jaar na afronden studie overgebracht naar het statische archief.	
Toepassingen		
Welke IT toepassing(en) worden ingezet ter ondersteuning van het proces? Vermeld hier ook eventuele alternatieven (pakket, systeem, netwerkcomponent e.d.).	Peoplesoft Campus Solutions	

Bijlage IV: Classificatievoorstel veel voorkomende gegevensobjecten

Ter indicatie bevat onderstaande tabel voor 25 veel voorkomende gegevensobjecten een voorstel voor de BIV classificatieniveaus.

Nr.	Data over	Komt volgens HORA voor in applicaties	Voorstel BIV
1.	Alumni	Komt voor als verwerking van instelling zelf en ook bij alumnivereenigingen.	MHM
2.	Betaaltransacties	Betaalsystemen	MMM
3.	Beelden cameratoezicht	Onderwijs Facilitair systeem	HMH
4.	Leden	Ledenadministraties	MMM
5.	Toetsen	Onderwijs	HHH
6.	Gediplomeerden	Examen register	LHM
7.	Debiteuren en crediteuren	Financieel systeem	MMM
8.	Leners	Bibliotheeksysteem Vertrouwelijkheid **hoog** indien de betaal- en leenhistorie wordt bewaard.	LHM/ LHH
9.	ICT gebruikers	Applicatieplatform: Identity management systeem	HHM
10.	Leveranciers	Bedrijfsvoering: Inkoopsysteem	LML
11.	Configuraties	Bedrijfsvoering: IT management systeem	LMH
12.	Kiesgerechtigden	Niet als zodanig in HORA aanwezig. Goed voorbeeld van **niet-bron** systeem: bevat informatie uit andere bronsystemen.	MHM
13.	Academische staf	Samenwerkingssysteem: Nevenwerk openbaar register (conform gedragscode NSVU)	LHL
14.	Onderzoeks-projecten	Onderzoeksgegevensbeheersysteem	LHM
15.	Medewerkers	Personeelssysteem	MHH
16.	Relaties	Bedrijfsvoering	MHH
17.	Roosters	Onderwijsondersteuning	HML
18.	Salarissen	Salaris verwerkingssysteem	MHH
19.	Sollicitanten	Als Medewerkers	MHH
20.	Studenten	Studenteninformatiesysteem Document Management Systeem Email Stage en afstudeer system	MHH
21.	Ruimten en gebruikers	Facilitair systeem: Toegang en beheersysteem	MMM
22.	Web content	Generiek	MMH
23.	Kengetallen	Management Informatie Systeem Indien anoniem, dan LML of LHL als ze de basis vormen van	LML LHH

Nr.	Data over	Komt volgens HORA voor in applicaties	Voorstel BIV
		grote bedrijfsbeslissingen. Indien niet anoniem dan de vertrouwelijkheid Hoog.	
24.	Cursussen, deelnemers	Digitale leeromgeving	MMM
25.	Mailberichten, mailadressen	E-mailsysteem	HHH