

CONCLUSION



RICHTLIJN DATA CLASSIFICATIE

Auteur

Roel Gloudemans
(roel.gloudemans@conclusion.nl)

Met medewerking van

Chris Gralike, Ricky Hoots, Artien Bel, Dennis
Pieterse, Paul Schoorl

Status: Definitief
Versie: 1.1 (22-02-2023 13:36:00)
Ten minste houdbaar tot: 2024-02-22

Versietabel			
Datum	Versie	Door	Aanpassing
21-09-13	0.1	R. Gloudemans	Eerste concept
22-02-04	1.0	R. Gloudemans	Definitieve versie
23-02-22	1.1	R. Gloudemans	Document nagelopen; geen wijzigingen

Accordering	
Document	Versie
Versie	1.0
<i>Alle hoofdversies van dit document worden geaccordeerd door minimaal 5 security officers van verschillende Conclusion bedrijven. Kleine wijzigingen, zoals spelfouten en wijzigingen en/of aanvullingen op de toelichting vinden plaats onder de verantwoordelijkheid van de Chief Security Officer van Conclusion</i>	
<i>Dit document is geclassificeerd als publieke informatie en kan (in pdf-vorm) beschikbaar worden gesteld aan iedereen voor wie dit beleidsstuk relevant is.</i>	

Inhoud

Pagina

1.	Samenvatting voor de medewerker	4
2.	Inleiding	5
2.1	Vindplaats	5
2.2	Achtergrond	5
2.3	Scope	5
2.4	Doelstelling	5
2.5	Doelgroep	5
3.	Classificatie	6
3.1	Wat is informatie classificatie	6
3.2	Conclusion classificatieschema	7
3.2.1	Voor documenten	7
3.2.2	Voor databronnen	8
3.2.3	Classificatie en veelgebruikte systemen	9
4.	Classificatieproces	10
5.	Classificatie en vertrouwen	11

1. Samenvatting voor de medewerker

Alle informatie binnen Conclusion moet geclassificeerd worden. Alleen zo kan geborgd worden dat de juiste hoeveelheid maatregelen genomen wordt en dat de veiligheidsmaatregelen niet overbodig lastig zijn.

Documenten worden alleen geclassificeerd op basis van vertrouwelijkheid. Hierbij worden de volgende classificaties gebruikt:

Classificatie voor vertrouwelijkheid en documenten		
Label	Verspreiding	Voorbeeld
Publiek	Mag door iedereen gezien worden	• Website • Beveiligingsbeleid
Bedrijfsgegevens	Mag alleen door Conclusion medewerkers gezien worden en een of meerdere klanten	• Conclusion dienstencatalogus
Intern	Mag alleen door een beperkte groep Conclusion medewerkers gezien worden en een beperkte groep medewerkers van een klant.	• Offerte • Lijst van genomen beveiligingsmaatregelen • Persoonsgegevens
Vertrouwelijk	Mag alleen door enkele Conclusion medewerkers gezien worden en enkele medewerkers van een klant.	• Aandeelhoudersinformatie • Financiële gegevens • Audit rapporten • Bijzondere persoonsgegevens

Deze classificaties kunnen in Office en de Mail ingesteld worden, waarna de bijbehorende maatregelen automatisch worden ingesteld.

Ben je verantwoordelijk voor een grotere (gestructureerde) dataset of een bedrijfsproces, dan moet de informatie die je verwerkt ook geclassificeerd worden op het gebied van Integriteit (correctheid & compleetheid) en beschikbaarheid. De betreffende labels hiervoor zijn te vinden op pagina 8.

Welke maatregelen in dat geval bij de classificatie horen zijn terug te vinden in de overige richtlijnen documenten die een hulpmiddel zijn voor de bouwers van infrastructuur, applicaties en processen en die een handvat bieden voor het beheersen van de risico's.

2. Inleiding

2.1 Vindplaats

Dit beleidsdocument en alle andere documenten waarnaar in dit document verwezen wordt zijn te vinden op de “Security”¹ pagina van Start Your Day.

2.2 Achtergrond

Niet alle informatie is even belangrijk voor Conclusion in termen van beschikbaarheid, integriteit en vertrouwelijkheid.

Informatieclassificatie is een methode om te bepalen hoe waardevol informatie is voor de bedrijfsprocessen en de belanghebbenden bij deze processen. Op basis van de classificatie wordt vastgesteld wat de standaard set van maatregelen is die voldoende zouden moeten zijn voor de bescherming van de belangen.

2.3 Scope

Dit document beschrijft de dataclassificatie, zoals deze wordt gebruikt wanneer er informatie wordt uitgewisseld tussen de Conclusion bedrijven en zoals het naar buiten gecommuniceerd wordt. Voor door dit doel is dit geïmplementeerd op de gemeenschappelijke KA omgeving.

2.4 Doelstelling

Dit document geeft aan wat de classificatie categorieën zijn, wanneer informatie in een bepaalde categorie valt, hoe de classificatie verloopt en wat de verantwoordelijkheden zijn.

2.5 Doelgroep

Dit document is bedoeld voor alle medewerkers, met de medewerkers die verantwoordelijk zijn voor grote informatiesets in het bijzonder.

Definities

Beschikbaarheid (continuïteit, responstijd).

De mate waarin de informatie binnen de organisatie beschikbaar moet zijn op het moment dat een gebruiker deze informatie nodig heeft.

Integriteit (juistheid, volledigheid, tijdigheid, geoorloofdheid).

De mate waarin de informatie binnen de informatiesystemen volledig en juist is. Hierbij geldt ook dat onder volledigheid dient te worden verstaan dat niet méér dan de benodigde informatie in het systeem is opgenomen.

Vertrouwelijkheid (exclusiviteit).

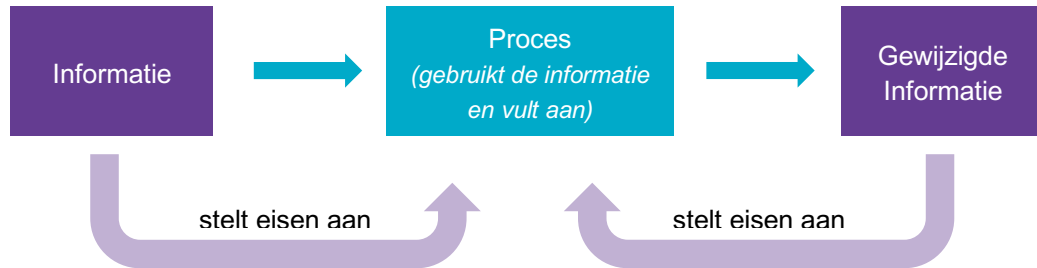
De mate waarin de toegang tot en de kennisname van de informatie beperkt is tot een gedefinieerde groep van gebruikers, die expliciet verklaard hebben op een juiste en zorgvuldige wijze om te zullen gaan met de informatiesystemen en de daarin opgenomen informatie.

¹ <https://conclusionfutureit.sharepoint.com/sites/StartYourDay/SitePages/Privacy-&-Security.aspx>

3. Classificatie

3.1 Wat is informatie classificatie

Het doel van informatie classificatie is om het belang van deze informatie aan te geven, zodat de verantwoordelijken voor informatie, proces, applicatie en infrastructuur maatregelen kunnen nemen om de informatie adequaat te kunnen beschermen. Deze maatregelen moeten er aantoonbaar voor zorgen dat Conclusion geen onacceptabele risico's neemt.



Figuur 1, Een bedrijfsproces dat informatie verwerkt.

Een bedrijfsproces heeft informatie nodig om te kunnen werken en produceert nieuwe informatie. Uit zowel de classificatie van de in- als uitvoer stellen eisen aan de maatregelen in het proces en de technologie die in het proces gebruikt wordt.

De informatieclassificatie legt het verband tussen het belang van de informatie en de minimale maatregelen die wenselijk zijn om dat belang te borgen.

Is een bepaalde maatregel niet aanwezig, dat wordt dat genoteerd als een kwetsbaarheid in het proces. Vervolgens wordt in een risicoanalyse bekeken of het in de context van het proces alsnog nodig is om de maatregel te nemen, of dat de afwezigheid van deze maatregel niet tot onacceptabele risico's leidt.

De aanbeveling is om de maatregel zo dicht mogelijk bij de informatie te nemen.

Door een vertrouwelijk Word bestand te versleutelen, kan het bijvoorbeeld in Teams opgeslagen worden en per mail verstuurd. Anders zou daar een speciale dienst voor ingericht moeten worden.

3.2 Conclusion classificatieschema

3.2.1 Classificatie overzichtstabel

Conclusion gebruikt een drie bij 4 matrix voor de classificatie. Hierbij is iedere cel gedefinieerd voor een vastgestelde term (publiek, correct, hoog,). Voor verwijzing naar de classificatie kan ook een niveau gebruikt worden. Het niveau wordt aangegeven met een getal.

Alle dataclassificatie niveaus van Conclusion			
Niveau	Beschikbaarheid	Integriteit	Vertrouwelijkheid
1	Zeer laag	Niet gecontroleerd	Publiek
2	Laag	Correct	Bedrijfsgegevens
3	Midden	Belangrijk	Intern
4	Hoog	Essentieel	Vertrouwelijk

3.2.2 Voor documenten

Documenten binnen Conclusion worden alleen maar geclassificeerd op vertrouwelijkheid. Integriteit en beschikbaarheid hebben wel betekenis, maar alleen voor de plaats waar de documenten worden opgeslagen en het proces om de informatie aan te passen daaromheen.

Classificatie voor vertrouwelijkheid en documenten		
Label	Verspreiding	Voorbeeld
Publiek	Mag door iedereen gezien worden	- Website - Beveiligingsbeleid
Bedrijfsgegevens	Mag alleen door Conclusion medewerkers gezien worden en een of meerdere klanten	Conclusion dienstencatalogus
Intern	Mag alleen door een beperkte groep Conclusion medewerkers gezien worden en een beperkte groep medewerkers van een klant.	- Offerte - Lijst van genomen beveiligingsmaatregelen - Persoonsgegevens
Vertrouwelijk	Mag alleen door enkele Conclusion medewerkers gezien worden en enkele medewerkers van een klant.	- Aandeelhoudersinformatie - Financiële gegevens - Audit rapporten - Bijzondere persoonsgegevens

Regels voor omgang met documenten					
#	Regel	Publiek	Bedrijfs- informatie	Intern	Vertr.
R-DC-1	Documenten zijn altijd voorzien van een classificatie	✓	✓	✓	✓
R-DC-2	Op het document is altijd aangegeven of het persoonsgegevens bevat			✓	✓
R-DC-3	De maker classificeert een document	✓	✓	✓	✓
R-DC-4	Verder verspreiden van het document moet gemeld worden bij de eigenaar.			✓	
R-DC-5	De ontvanger mag een document niet verder verspreid worden.				✓
R-DC-6	Afwijken/veranderen van de classificatie moet gemeld wordt bij de eigenaar.			✓	
R-DC-7	De ontvanger mag de classificatie niet veranderen.				✓
R-DC-8	Bij persoonsgegevens moet de bewaartermijn op het document vermeld worden ² .			✓	✓

3.2.3 Voor databronnen

Voor informatie in databases en andere soorten van informatieopslag gelden naast de classificatie voor vertrouwelijkheid ook nog de classificaties voor integriteit en beschikbaarheid. Indien deze classificaties wel belangrijk zijn voor een document, dient het bedrijfsproces ervoor te zorgen dat het document wordt opgeslagen in een informatiebron die de juiste maatregelen heeft genomen op het vlak van integriteit en beschikbaarheid.

De maatregelen behorende bij iedere classificatie zijn terug te vinden in de diverse richtlijnen documenten.

Classificatie voor integriteit		
Label	Beschrijving	Voorbeeld
Niet gecontroleerd	Ongecontroleerde wijziging van de informatie heeft geen negatieve effecten.	Interne nieuwsbrief
Correct	Er moet met enige zekerheid gesteld kunnen worden dat de informatie correct en volledig is. Verkeerde of onvolledige informatie leidt tot verwarring.	- Loonstrook - Audit rapport - Website
Belangrijk	Het is van belang dat de informatie correct is. Incorrecte informatie leidt	- Offerte - Persoonsgegevens

² Zie "Richtlijn Bewaartermijnen" voor hulp bij het vaststellen van de bewaartermijn

	tot schade bij Conclusion of een enkele klant of betrokkene.	
Essentieel	Het niet correct of volledig zijn van de informatie leidt tot onomkeerbare schade voor Conclusion en een of meerdere klanten of betrokkenen.	• Bijzondere persoonsgegevens • Grote financiële transacties

Classificatie voor beschikbaarheid		
Label	Beschrijving	Voorbeeld
Zeer laag	Het is niet erg als de informatie niet beschikbaar is.	• Foto's van het laatste teamuitje
Laag	Informatie waarbij men ervan uitgaat dat deze beschikbaar is, maar waarbij de activiteiten kunnen wachten.	• Start Your Day
Midden	Informatie waarbij men ervan uitgaat dat deze beschikbaar is, maar waarbij de activiteiten niet lang kunnen wachten.	• Website • Financiële administratie • Teams
Hoog	Informatie ter ondersteuning van vitale processen van klanten of Conclusion.	• Verkeersgegevens van de NS.

3.2.4 Classificatie en veelgebruikte systemen

Geschiktheid van veelgebruikte opslagmedia			
Voorziening	Vertrouwelijkheid	Integriteit	Beschikbaarheid
Teams	Bedrijfsinformatie	Correct	Midden
Teams met versleutelde bestanden	Vertrouwelijk	Belangrijk	Midden
e-Mail	Bedrijfsinformatie	Niet gecontroleerd	Laag
e-Mail versleuteld	Vertrouwelijk	Belangrijk	Laag
USB-stick	Bedrijfsinformatie	Niet gecontroleerd	Zeer laag
Laptop	Bedrijfsinformatie	Correct	Laag

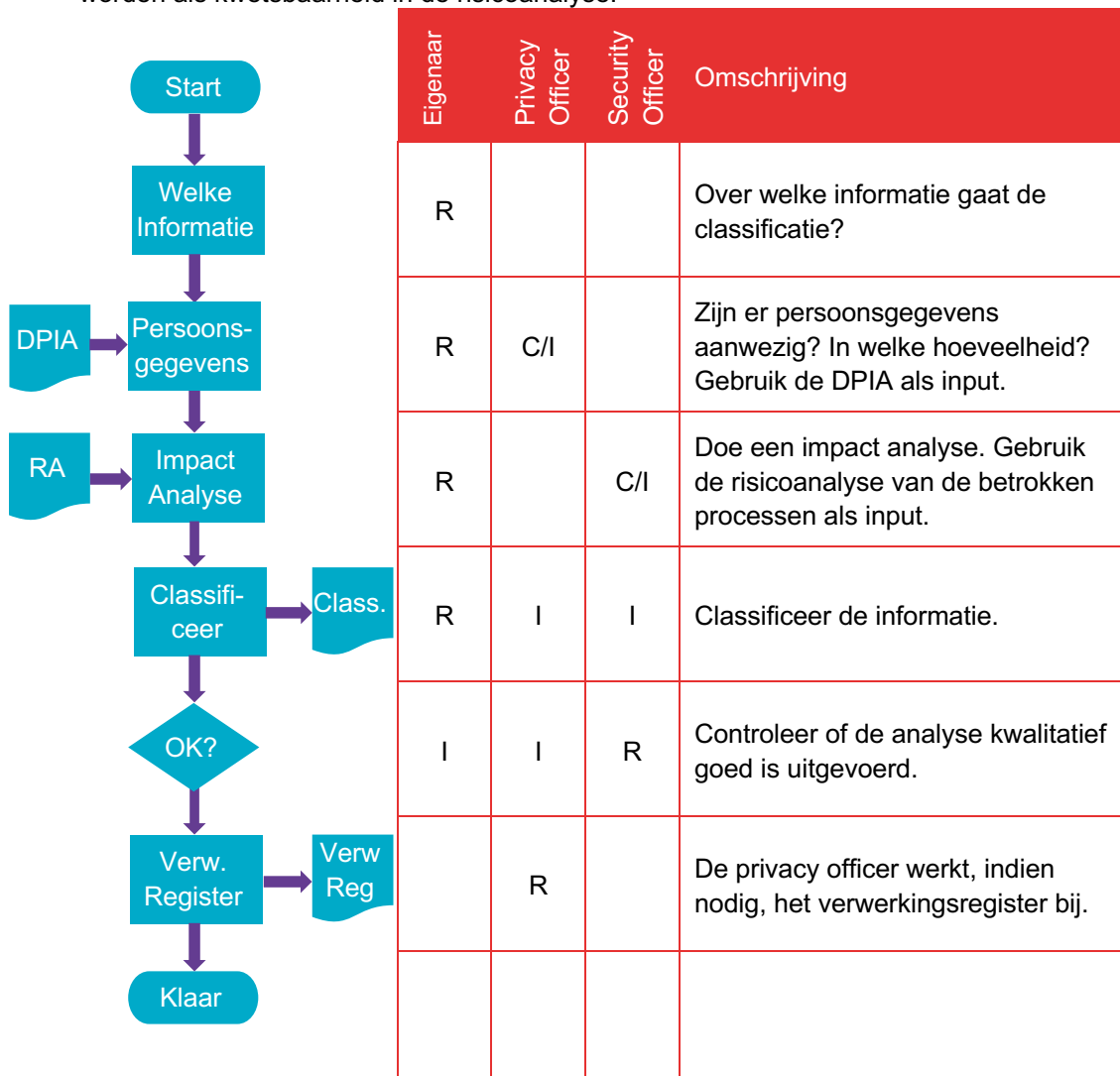
4. Classificatieproces

Classificatie van informatie is een belangrijk hulpmiddel voor het bepalen van de juiste maatregelen om de informatie te beschermen. In de praktijk worden er vaker te veel maatregelen genomen, dan te weinig. Dit resulteert in complexe handelingen, ergernis en kosten.

Bij de classificatie van informatie zijn een aantal spelers betrokken. De belangrijkste daarvan is de verantwoordelijke voor de informatie, een rol die vaak aangeduid wordt met "eigenaar". De eigenaar is verantwoordelijk voor een correcte classificatie en dient erop toe te zien dat de informatie goed beschermd wordt. Hierbij wordt de eigenaar geholpen door de security en privacy officers.

Documenten worden geclassificeerd door de maker, of krijgen een classificatie mee vanuit het bedrijfsproces waarin zij gegenereerd worden, bijvoorbeeld een loonstrook.

De eigenaar van de informatie moet erop toezien dat de verantwoordelijken voor processen en systemen de juiste maatregelen nemen om de informatie te beschermen. Maatregelen die niet genomen zijn, dienen genoteerd te worden als kwetsbaarheid en dienen door de verantwoordelijken voor de betrokken bedrijfsprocessen meegenomen te worden als kwetsbaarheid in de risicoanalyse.



5. Classificatie en vertrouwen

Informatie wordt verwerkt op een locatie. Deze locatie is fysiek en/of digitaal. Een kenmerk van een locatie is op deze vertrouwd wordt of niet. Hierbij zijn er drie mogelijkheden:

1. Een vertrouwde locatie, hieronder vallen vertrouwde applicaties en infrastructuur van Conclusion (zie het “Beveiligingsbeleid Ecosysteem” document voor de definitie van vertrouwen).
2. Een gecontroleerde locatie, die niet vertrouwd is maar waarin wel sprake is van veiligheidsmaatregelen. Hieronder vallen de applicaties en infrastructuur waar Conclusion wel invloed op uit kan oefenen, maar die niet vertrouwd zijn. Een ander voorbeeld is bijvoorbeeld een partij waarmee Conclusion een verwerkersovereenkomst heeft afgesloten;
3. Een niet vertrouwde locatie, dit zijn de applicaties en infrastructuur waar Conclusion geen invloed wil en/of kan uitoefenen en die niet vertrouwd zijn. In het fysieke domein zijn dit bijvoorbeeld openbare locaties.

Indien informatie met een bepaalde classificatie vanuit in een niet geschikte locatie verwerkt moet worden, dienen er additionele maatregelen getroffen te worden.

		Locatietype waar de informatie verwerkt mag worden
Integriteit	Niet gecontroleerd	Niet vertrouwd
	Correct	Gecontroleerd
	Belangrijk	Vertrouwd
	Essentieel	Vertrouwd
Vertrouwelijkheid	Publiek	Niet vertrouwd
	Bedrijfsinformatie	Gecontroleerd
	Intern	Gecontroleerd
	Vertrouwelijk	Vertrouwd

CONCLUSION

CONTACT

Roel Gloudemans
Chief Security Officer
roel.gloudemans@conclusion.nl
+31-6-13372217