

Richtlijnen - Beveiligen van Gegevens obv Classificatie

ISO27002

Inhoudsopgave

1	Doel	2
2	Herziening van het document	2
3	Eisen	2
4	Beleid rond het beveiligen van gegevens – Vereisten	3
4.1	Context	3
4.2	Classificatie van gegevens.....	3
4.3	Labelen van informatie	4
4.4	Behandelen van informatie	4
4.4.1	Klasse 1 : Publieke gegevens	4
4.4.2	Klasse 2 : Interne bedrijfsgegevens.....	4
4.4.3	Klasse 3 : Vertrouwelijke bedrijfsgegevens	4
4.4.4	Klasse 4 : Persoonsgegevens	5
4.4.5	Klasse 5 : Vertrouwelijke persoonsgegevens	5
4.4.6	Klasse 6 : Gevoelige persoonsgegevens	5

		Datum
Auteur:	IT Informatiebeveiliging - CISO	2024-12-06
Goedkeuring:	Directeur ICT	2024-12-06
Voor de versiegeschiedenis verwijzen we naar het document management system.		

1 Doel

Het doel van dit beleid is om een raamwerk vast te stellen voor het classificeren van Pidpa-gegevens die worden verwerkt op basis van het niveau van gevoeligheid, waarde en criticiteit zoals vereist door het informatiebeveiligingsbeleid. De classificatie van gegevens helpt bij het bepalen van de basisbeveiligingscontroles voor de bescherming van deze gegevens.

2 Herziening van het document

Om te garanderen dat het document in lijn is met de actuele situatie zal het document periodiek herzien worden. Voor deze procedure is dit jaarlijks of bij significante wijzigingen binnen de organisatie.

3 Eisen

ISO27002:2022 - A.5.12 Classificeren van informatie

ISO27002:2022 - A.5.13 Labelen van informatie

4 Beleid rond het beveiligen van gegevens – Vereisten

4.1 Context

Informatie kan vele vormen aannemen, waaronder, maar niet beperkt tot, de volgende:

- Gegevens op papier
- Gegevens die elektronisch zijn opgeslagen in computersystemen
- Communicatie verzonden per post of e-mail
- Gegevens opgeslagen op elektronische media zoals USB-sticks, schijven en tapes

Persoonlijke informatie is alle informatie over een identificeerbare persoon. Pidpa is hier wettelijk verantwoordelijk voor en de opslag, bescherming en het gebruik ervan zijn onderworpen aan nationale en internationale wetgeving.

Pidpa houdt een inventaris bij van alle belangrijke informatiemiddelen waarop zij vertrouwt. Pidpa erkent echter dat er risico's zijn verbonden aan werknemers, klanten, aannemers en andere derden die toegang krijgen tot informatie en ermee omgaan om officiële organisatiezaken uit te voeren.

Pidpa heeft de verantwoordelijkheid om de informatie die zij bewaart en verwerkt te beschermen door middel van controles die zijn afgestemd op de gevoeligheid van de betreffende informatie.

Alleen door informatie te classificeren volgens een gedocumenteerd schema kan het juiste beschermingsniveau worden toegepast. Deze procedure beschrijft de details van de te gebruiken regeling en de criteria die worden toegepast om te beslissen welk beschermingsniveau moet worden toegepast op een bepaald informatiemiddel.

Deze controle is van toepassing op alle systemen, mensen en processen die de informatiesystemen van de organisatie vormen, met inbegrip van bestuursleden, directeuren, werknemers, leveranciers en andere derden die toegang hebben tot de systemen van Pidpa.

Pidpa beheert heel wat persoonlijke en financiële gegevens van klanten en personeelsleden. Zij stellen hun vertrouwen in Pidpa voor de veilige verwerking en omgang met deze persoonlijke gegevens. Indien dit vertrouwen geschaad wordt, staat de reputatie van Pidpa op het spel.

Het is daarom ieders taak om uiterst zorgvuldig met deze informatie om te gaan en criminelen geen kans te geven om deze te bemachtigen of te manipuleren.

Daarenboven kent de Europese GDPR wet- en regelgeving zware sancties bij inbreuken.

4.2 Classificatie van gegevens

De classificatie van gegevens naar vertrouwelijkheid gebeurt op basis van de betekenis of inhoud (content) van de gegevens. Het is immers de content die bepalend is voor de schade die opgelopen wordt indien de gegevens in verkeerde handen vallen. Voor de gegevens die informatie over personen bevatten is bijzondere aandacht nodig omdat deze onder de wet op de privacy vallen.

Klasse 1 - Publieke gegevens : de gegevens die openbaar zijn of geen vertrouwelijke inhoud hebben. Een voorbeeld hiervan zijn de publieke gegevens op de website van Pidpa.

Klasse 2 - Interne bedrijfsgegevens : de gegevens waarvan het gebruik beperkt moet worden tot binnen het bedrijf. Deze gegevens zijn niet bestemd voor publieke bekendmaking zonder voorafgaande goedkeuring door de directie. In principe vallen hier alle gegevens onder die aanwezig zijn in Pidpa-documenten of ingebracht in ICT-systemen.

Klasse 3 - Vertrouwelijke bedrijfsgegevens : dit zijn de bedrijfsgegevens die ofwel binnen de context van Pidpa of de partners een vertrouwelijk karakter hebben. Deze gegevens zijn niet bestemd voor verspreiding, noch binnen noch buiten het bedrijf, zonder voorafgaande goedkeuring van de beheerder van de gegevens of de directie. Het kan hier gaan over de meest diverse gegevens als financiële gegevens, operationele gegevens, commerciële gegevens, enz.

Klasse 4 - Persoonsgegevens : een persoonsgegeven is iedere informatie over een geïdentificeerd of identificeerbaar natuurlijk persoon. Alle persoonsgegevens hebben een min of meer vertrouwelijk karakter en zijn gebonden aan de richtlijnen uit de wet op de privacy. Ook ogenschijnlijk triviale gegevens als vb. naam, adres en telefoonnummer zijn persoonsgegevens.

Klasse 5 - Vertrouwelijke persoonsgegevens : dit zijn de persoonsgegevens die een vertrouwelijk karakter hebben. Voor deze gegevens hebben we ons te houden aan de privacywet (cf. persoonsgegevens), maar eveneens aan bijzondere bijkomende behandeling ter bescherming ervan. Voorbeelden hiervan zijn gegevens i.v.m. verloning, evaluaties, wanbetalers, enz...

Klasse 6 - Gevoelige persoonsgegevens : het gaat om gegevens over ras, politieke opvattingen, godsdienstige of levensbeschouwelijke overtuigingen, lidmaatschap van een vakvereniging, gezondheid, seksuele leven, verdenkingen, vervolgingen, strafrechtelijke of bestuurlijke veroordelingen. De wetgever heeft bepaald dat het verboden is om dergelijke gegevens te verwerken.

In deze classificatie zijn, met uitzondering van de publieke gegevens (klasse 1) en interne bedrijfsgegevens (klasse 2), alle gegevens vertrouwelijk. Voor deze vertrouwelijke gegevens zijn extra maatregelen van toepassing, afhankelijk van de klasse.

4.3 Labelen van informatie

Elk document dat in het documentbeheersysteem van Pidpa wordt opgeslagen dient verplicht voorzien te worden van zijn classificatieniveau.

4.4 Behandelen van informatie

Voor elk classificatieniveau gelden algemene gegevensverwerkingsregels voor het opslaan, delen en verwijderen van informatie.

4.4.1 Klasse 1 : Publieke gegevens

- Geen beperkingen

4.4.2 Klasse 2 : Interne bedrijfsgegevens

- Toegang tot deze gegevens wordt verleend op basis van het principe van minimale privileges ("Principle of Least Privilege").
- Waar mogelijk dienen deze gegevens versleuteld te worden opgeslagen en verstuurd.
- Afdrukken, doormailen of kopiëren van documenten mag uitsluitend voor intern gebruik; anders is toelating van de verantwoordelijke vereist.
- Deze gegevens dienen veilig te worden verwijderd, om te zorgen dat reconstructie niet mogelijk is.

4.4.3 Klasse 3 : Vertrouwelijke bedrijfsgegevens

- Alle verwerkingsregels van Klasse 2 zijn van toepassing.
- Versleuteling van datatransport wordt toegepast om af luisteren te voorkomen.
- De gegevens mogen niet op mobiele apparaten (laptop, USB, CD, ...) worden geplaatst zonder versleuteling ervan (encryptering) of een beveiliging via toegangscode.

- Afgedrukte documenten mogen niet onbeheerd achtergelaten worden op de werkplek. Voor deze documenten geldt dus het 'clean desk'-principe.
- Afgedrukte documenten mogen niet zomaar in de prullenmand belanden. Vernietiging is verplicht.

4.4.4 Klasse 4 : Persoonsgegevens

- Alle verwerkingsregels van Klasse 3 zijn van toepassing.
- De wetgeving op de privacy is van toepassing. Alle medewerkers moeten hiervan op de hoogte gebracht worden.

4.4.5 Klasse 5 : Vertrouwelijke persoonsgegevens

- Alle verwerkingsregels van Klasse 4 zijn van toepassing.
- Afdrukken, doormailen of kopiëren van deze documenten is niet toegelaten tenzij voor specifieke doeleinden. Hiervan is een inventaris beschikbaar bij de verantwoordelijke, bevattende de gemandateerde(n).
- Afgedrukte documenten moeten achter gesloten deur bewaard worden. Dit geldt ook voor archieven.
- Afgedrukte documenten mogen het gebouw niet verlaten zonder bijkomende maatregelen. Er moet steeds toezicht zijn op het document tot aan de bestemming.
- De toegang tot deze gegevens is traceerbaar op gebruikersnaam of is afgeschermd tot een beperkt aantal geïdentificeerde personen.

4.4.6 Klasse 6 : Gevoelige persoonsgegevens

- Verwerken van deze gegevens is niet toegelaten.