Federal Information Security Policy Guideline

Handleiding voor logging

21/11/2019

FISPDOC04 V1.2

Belangrijke opmerking: Dit document is een leidraad die het resultaat is van een samenwerking tussen informatiebeveiligingsexperts van de verschillende federale diensten (FOD, OIP, IPSS). De voorgestelde maatregelen worden beschouwd als minimummaatregelen die redelijkerwijs op een gemeenschappelijke manier van toepassing zijn op alle federale diensten. Deze zijn gebaseerd op internationale normen, goede praktijken op het gebied van informatiebeveiliging en de ervaringen van de deelnemers aan de FISP-werkgroep.

Indien strengere maatregelen vereist zijn voor een federale dienst omwille van reglementaire redenen of om andere formele en dwingende redenen, kan men ervan uitgegaan dat deze maatregelen voorrang hebben op de maatregelen die in deze gids worden beschreven.

FISP Werkgroep

.be

Inhoudstafel

I. Inhoud van dit document 2
Oriëntatie van het document 3
Veiligheidsdoel van het document 3
Toepassingsgebied 3
Vertrouwelijkheid van het document 3
Vrijwaring 3
Verantwoordelijkheden 3
Eigenaar 3
II. De FISP werkgroep is de eigenaar van dit document. 3
III. Inleiding 4
IV. Logging 5
Logging als beveiligingsmaatregel 5
Het doel van logging 5
De bron van logging 5
De logbestanden 6
V. Informatieclassificatie - Logging 7
Algemene maatregelen 7
VI. Logbeheer 9
Algemene Log maatregelen 9
Specifieke extra maatregelen voor privacy logs 10
VII. Manuele logboeken 11
VIII. Retentie en beveiliging van audit records 11
IX. Opslag management 11
X. Omgaan met fouten in auditing 12
XI. Audit opvolging, analyse en rapportering 12
XII. Link met andere maatregelen 13
Link met PAM als maatregel 13
Link met cryptografische maatregelen 13
XIII. Documentbeheer 13
Historiek 13
Goedkeuringen 13
Bronnen 13
XIV. Link met een ander beleid 14
Afhankelijkheid van interne documenten 14
Positionering van het beleid t.o.v. de ISO 27001-norm 14
Positionering van het beleid t.o.v. de ISO 27002-norm 14

Inhoud van dit document

Oriëntatie van het document

Dit document maakt integraal deel uit van methodologie voor informatiebeveiliging binnen de Federale overheid (FISP-project).

Iedere federale organisatie dient te beschikken over een beleid en processen inzake het gebruik van logging.

Veiligheidsdoel van het document

Dit beleid is geschreven om informatiebeveiligingsmaatregelen met betrekking tot logging aan te reiken, zodat invulling gegeven kan worden aan het beveiligingsbeleid.

Toepassingsgebied

Dit beleid is geen volledige procesbeschrijving voor logging en bevat geen productbeschrijvingen, maar bevat wel voldoende informatie om goede (beleid)keuzes te maken en bewustwording te creëren met betrekking tot logging.

Vertrouwelijkheid van het document

Publieke verspreiding

Vrijwaring

Dit is een beleid op basis van de internationale praktijken m.b.t. logging. Indien u deze richtlijn voor uw organisatie wilt toepassen, moet u eerst een beoordeling maken en controleren of andere wettelijke beperkingen, regels of praktijken van toepassing zijn op uw organisatie. Pas het beveiligingsbeleid aan, in lijn met uw organisatie!

Tijdens de Ministerraad van 3 mei 2019 werd een voorontwerp van wet voorgelegd, namelijk de herziening van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen. Indien deze wet wordt aangenomen, zal het FISP beleid worden geüpdatet aangezien het huidige beleid geen rekening houdt met toekomstige wettelijke ontwikkelingen.

Verantwoordelijkheden

Dit document is bestemd voor de informatieveiligheidsconsulent (CISO) en voor de functionaris voor de gegevensbescherming (DPO) van de openbare instelling van federale overheid, voor de verwerkers van informatie (ook de onderaannemers van informatiesystemen), de veiligheidsofficier en andere belanghebbenden in verwante gebieden (bv. de documentenbeheerder).

Eigenaar

De FISP werkgroep is de eigenaar van dit document.

Inleiding

Informatiesystemen en ICT-infrastructuur genereren log-informatie voor veel activiteiten, soms als normale statusmelding, soms als resultaat van een activiteit van een gebruiker of beheerder maar ook informatie als resultaat van onvoorziene omstandigheden of fouten.

Dit beleid biedt informatiebeveiligingsmaatregelen aan met betrekking tot logging voor de federale organisaties. Het document bevat de nodige informatie om goede (beleid)keuzes te maken en bewustwording te creëren. De voorgestelde maatregelen zijn gekoppeld aan de voorgestelde informatie classificatie van het federale informatiebeveiligingsbeleid (FISP).

Er wordt bovendien advies gegeven in de maatregelen die men moet nemen voor logbeheer. Daarnaast worden er ook aanwijzingen gegeven over de retentie en beveiliging van audit records, hoe om te gaan met fouten in audit records en audit opvolging, analyse en rapportering.

Het is echter geen volledige procesbeschrijving voor logging en monitoring en bevat ook geen productbeschrijving. Een uitgebreide beschrijving betreffende het principe logging en monitoring kan men terug vinden in het FISP document “Logging & monitoring” –Verklaring”.

Logging

Logging als beveiligingsmaatregel

Audit log en audit trails zijn een belangrijke beveiligingsmaatregel op zichzelf. Het werkt namelijk preventief wanneer men door het opvolgen van informatie uit audit logs de eerste signalen van een cyberaanval kan herkennen. Hierna kunnen dan de nodige stappen ondernomen worden om deze aanval te stoppen en/of verdere gevolgen te voorkomen.

Het werkt echter ook reactief doordat men door log analyse en correlatie met andere informatiebronnen kan achterhalen wat er precies gebeurd is. Logging kan reactief een ondersteuning bieden voor het proces van risico beheer. Het kan gebruikt worden ter ondersteuning van het proces probleembeheer. Men kan het gebruiken om te leren uit incidenten en het kan dienst doen voor bewijsvoering – juridische bewijsvoering. Tot slot is het ook handig voor het statistisch gebruik.

Het doel van logging

Er zijn echter verschillende reden (conformiteit, statistisch en operationeel) waarom een organisatie kan beslissen om een log te creëren:

- detectie van verdacht gedrag (misbruik intern, ongeautoriseerde toegang, hacking, …) en cyber aanvallen
- support voor forensische analyse en correlatie
- bewijsverschaffing (verzamelen van bewijsmateriaal, fraudeopsporing…)
- conformiteit met geldende regelgeving
- support business processen (rapportering, …),
- support IT onderhoud & operations
- debugging, testen
- performantie monitoring, van applicaties en systemen
- …

De bron van logging

Echter niet alleen het doel van logging maar ook de bron van log events is van essentieel belang. De bronnen voor een log kunnen heel divers zijn :

- Applications (Gebruikersaccount informatie, Operationele acties, Data manipulatie, Informatie gebruik)
- Netwerk (routers, switches, AP, …)
- Security software en appliances (IDS.IPS, Firewalls, antimalware software, Remote access (VPN), Web proxies, authentication services, vulnerability management software, network quarantine servers, …)
- Servers and databases
- Middleware (ESB, …)
- Besturingssystemen (fix/mobile) System events, audit records
- Randapparatuur: MFP, …
- datacentrum & gebouw (badges, HVAC, monitoring …)
- Virtuele omgevingen: (virtuele servers, netwerken, hypervisors, …)
- LAN applicaties
- …

Weten waarom de log is opgezet en wat de bron van het logevent is, is cruciaal. Het bepaalt namelijk in zekere mate ook de soort beveiligingsmaatregelen die genomen moeten worden. Zo zullen de beveiligingsmaatregelen voor logging betreffende support in IT onderhoud verschillen met deze voor een detectie van verdacht gedrag. Een log event dat voorkomt uit applicaties of uit security software verschilt eveneens in beveiligingsmaatregelen. De beveiligingsmaatregelen moeten bijgevolg in lijn zijn met de reden van logging en de bron van het log event.

De logbestanden

Er is ook de informatie die door de log beschermd wordt. Logbestanden moeten beveiligd worden tegen niet-geautoriseerde toegang. De log zelf moet dezelfde informatiecategorie toegewezen krijgen als de informatiecategorie van de informatie die ze beschermt. Aangezien deze informatie opgenomen is in de logs moeten de bijhorende maatregelen ook op de log informatie toegepast worden. Dit geldt vooral voor applicatie logs en in mindere mate voor systeem logs, omdat deze laatste meestal geen applicatieve informatie bevatten.
De logbestanden kunnen de volgende bestanden omvatten: ID's, systeem activiteiten, datums, tijden, details over events, het gebruik van privileges, netwerk adressen,…
Log bestanden kunnen dus ook persoonlijke en gevoelige informatie beschermen. Voor deze privacy logs moeten de gepaste privacy maatregelen genomen worden.

Volgende maatregelen zouden moeten worden toegepast om de vertrouwelijkheid, integriteit en beschikbaarheid van log informatie te garanderen doorheen de volledig levenscyclus van de log informatie:

Vertrouwelijkheid:

- Fysieke of logische toegangscontrole;
- Encryptie van de log informatie.

Integriteit:

- 'read only' toegang tot log informatie verzekeren;
- Functiescheiding toepassen;
- Log informatie centraal opslaan;
- Time stamping en digitaal tekenen.

Beschikbaarheid:

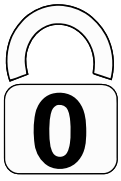
- Log informatie centraal opslaan;
- Back-up nemen van logbestanden;
- Logging opnemen in DRP (disaster recovery plannen).

Informatieclassificatie - Logging

Algemene maatregelen

Logging en de beveiliging van logbestanden zouden moeten georganiseerd worden in lijn met de voorgestelde informatie classificatie van dit globale informatiebeveiligingsbeleid (FISP). De voorgestelde maatregelen zijn gestapelde maatregelen. Dit impliceert dat de maatregelen van de onderliggend informatieklasse ook op de bovenliggende klassen van toepassingen blijven, met uitzondering van onverenigbare technische maatregelen. Bovendien evolueert de complexiteit en sterkte van de maatregelen mee met de stijging van de klasse.

Categorie	

	• Gebruik van geprivilegieerde accounts.
	• Applicatie logs: cryptografische maatregelen i.v.m. log informatie staan op hetzelfde niveau als de toepassing waaruit de log info aangemaakt wordt.
	• Logging van gebeurtenissen:
	  ○ Log policy opzetten voor alle systemen en toepassingen,
	  ○ logging opzetten ter ondersteuning van het incident proces:
	  ▪ Type gebeurtenis,
	  ▪ Waar en wanneer de gebeurtenis plaats vond,
	  ▪ Oorzaak en gevolg van de gebeurtenis,
	  ▪ Accounts gelinkt aan de gebeurtenis.
	• Monitoring van clear log gebeurtenissen
	• Lokale opslag van log informatie.
	• Beschermen van audit records om de integriteit te garanderen.
	• Timestamps op audit records d.m.v. een toepassing van kloksynchronisatie.
	• Toegang tot audit records beperken tot consultatie functie (‘read only’).

	• Beschermen van audit record om niet enkel de integriteit maar ook de vertrouwelijkheid te garanderen d.m.v. fysieke beveiliging en logische toegangscontrole. • Opzetten audit trail voor verwerking van informatie en het gebruik van systeemhulpmiddelen. • Timestamps op audit records d.m.v. een toepassing van kloksynchronisatie met een goedgekeurde externe tijdsbron. • Periodieke analyse van audit records. • Gebruik maken van tools voor analyse en rapportering • Jaarlijks de audit functie evalueren. • Ook over loggen moet worden gelogd: ○ het openen van een nieuw logbestand, het verplaatsen, wijzigen naam of verwijderen van een logbestand, het inkijken, verwijderen of wijzigen van de inhoud van een logbestand dient te worden gelogd om niet-geautoriseerde toegang te kunnen opsporen. • Centrale opslag van loginformatie. • Retentieperiode van lokale loginformatie beperken tot caching (tot centrale opslag geverifieerd gelukt is). • Alarmen genereren en opvolgen als opslagcapaciteit voor logbestanden 80% bereikt heeft. • lange termijn bewaring/archivering van log informatie conform wet- en regelgeving.

	• Er werden geen extra maatregelen geïdentificeerd voor informatie categorie 2.
	• Beschermen van audit record om niet enkel de integriteit maar ook de vertrouwelijkheid te garanderen d.m.v. cryptografische maatregelen. • Logging integreren met scanning en monitoring capaciteiten. • Timestamps in combinatie met digitale handtekening toepassen. • Event correlatie toepassen. • Centraal beheer van logbestanden • Real-time alarmen genereren en opvolgen bij problemen met de audit functie. • 4-ogen principe toepassen bij elke wijziging aan de audit functionaliteit.
	• Er werden geen extra maatregelen geïdentificeerd voor informatie categorie 4. • Men dient voor deze categorie rekening te houden met andere veiligheidseisen op basis van de wet van 11/12/1998.

Logbeheer

De maatregelen voorgesteld in dit hoofdstuk zijn minimaal voor logbeheer. Elke federale organisatie werkt de volgende beleidslijnen uit betreffende informatieveiligheid en privacy voor alle informatie en informatiesystemen onder de verantwoordelijkheid van de federale organisatie.

Algemene Log maatregelen

- De organisatie dient een formele procedure van logbeheer op te zetten, te valideren, te communiceren en te onderhouden:
    - een werkend log system;
    - de controle op de naleving van de procedure en op de inhoud van de logbestanden;
    - het beheren, het bewaren, het archiveren en het verwijderen van de informatieveiligheids- en privacy-logbestanden na het verstrijken van de bewaarduur ervan;
    - de beslissing om de loggegevens op te nemen in het continuïteitsplan van de organisatie;
    - de gecontroleerde toegang tot de loggegevens;
    - de organisatie moet als eigenaar van de toepassing de informatieveiligheids- en privacy-logbestanden voorzien en beheren. Bijvoorbeeld op het niveau van de transactionele monitor, het besturingssysteem, het beheersysteem van de machtigingen, het beheer en de bijwerking van de gegevensbanken;
    - de organisatie moet periodiek controles verrichten om de naleving van de maatregelen die op haar betrekking hebben te vergewissen;
    - De rollen en verantwoordelijkheden binnen de organisatie aangaande logbeheer moeten duidelijk zijn gedefinieerd. Waar mogelijk zou men moeten verhinderen dat systeem administrators de mogelijkheid hebben om eigen logs te deactiveren of verwijderen betreffende hun eigen activiteiten.
- De organisatie zou transacties, controlewerkzaamheden, activiteiten van gebruikers, uitzonderingen en informatieveiligheid- en privacy-gebeurtenissen/incidenten gestructureerd moeten vastleggen in afzonderlijke logbestanden, zodat iedere handeling naar de brondocumenten herleid kan worden of uitgevoerde bewerking(en) gecontroleerd kan worden.
- Logbeheer zou meegenomen moeten worden vanaf het design tijdens de ontwikkeling of bij de bepalingen van aankoopcriteria van toepassingen of systemen om “security/privacy by design” te realiseren.
- Elke toegang tot gegevens met gevoeligheidscategorie vertrouwelijk of hoger, zou gelogd moeten worden in overeenstemming met de toepasselijke wetgeving en regelgeving.
- De interne klokken van alle informatiesystemen van de organisatie dienen gesynchroniseerd te worden met een overeengekomen nauwkeurige tijdsbron opdat een betrouwbare analyse van logbestanden op verschillende informatiesystemen altijd mogelijk is.
- De noodzakelijke tools zouden beschikbaar moeten zijn of ontwikkeld worden om log gegevens te kunnen uit te baten en te laten analyseren door de geautoriseerde personen. Via de tools moet het mogelijk zijn om de logs snel, glashelder en eenvoudig te kunnen raadplegen.
- Waar mogelijk wordt systeemgebruik automatisch gelogd, als dit niet mogelijk is kan ook gebruik gemaakt worden van een manueel logboek door systeembeheerders.
- Logbestanden dienen beschermd te worden tegen inzage door onbevoegden, wijzigingen en verwijderingen.

- De logbestanden zouden moeten bewaard worden gedurende een overeengekomen periode, ten behoeve van toekomstig onderzoeken en controles en in overeenstemming met wetgeving en regelgeving.
- De organisatie van logbeheer omvat ook de uitvoering van alle taken die borg staan voor een duurzaam beheer van alle logbestanden gedurende de levenscyclus van de log. Bijzondere aandacht wordt besteed aan de volgende aspecten:
    - de beveiligde inzameling,
    - de bewaring en de archivering in een bruikbaar formaat en op bruikbare dragers die elk risico op vervalsing tot een minimum beperken,
    - de alarmprocedure wanneer belangrijke feiten zoals de onmogelijkheid om de logbestanden te traceren, aan het licht worden gebracht,
    - de controle naar de integriteit van de geïmplementeerde maatregelen,
    - de beheerprocedures.
- De raadpleging van logbestanden is altijd het voorwerp van een georganiseerde procedure binnen de organisatie met een historiek van de verzoeken die werden goedgekeurd/uitgevoerd of die werden afgekeurd.
- Het resultaat van logbeheer zou men regelmatig moeten analyseren, rapporteren en beoordelen.

Specifieke extra maatregelen voor privacy logs

- De privacy logs moeten bewaard worden gedurende een overeengekomen periode, ten behoeve van toekomstig onderzoeken en controles en in overeenstemming met wetgeving en regelgeving.[1]
- De kwaliteit van de privacy log dient een gepast antwoord te bieden om het gebruik te rechtvaardigen (al dan niet gebaseerd op een voorafgaandelijke autorisatie of machtiging). De log dient per verwerking een aanduiding te bevatten van:
    - wie wanneer persoonsgegevens heeft verwerkt,
    - op wie de persoonsgegevens betrekking hebben,
    - voor welke doeleinden de persoonsgegevens verwerkt moeten worden,
    - met welk beoogd resultaat de verwerking plaatsvindt (OK,NOK).

  In het logbeheer van privacy logs zouden minimaal de volgende zes vragen beantwoord moeten worden:
    - Welke activiteit had plaats? (Wat) (operatie)
    - Wanneer gebeurde de activiteit? (Wanneer) (Datum/tijd)
    - Wie voerde de activiteit uit? (Welke organisatie) (Wie)
    - Met welk systeem gebeurde de activiteit? (Hoe) (Applicatie ID)
    - Op welk object voerde de activiteit iets uit? (Over wie) (De betrokkene van de verwerking)
    - Wat was het resultaat/de status van de activiteit? (Gelukt / mislukt)

  De volgende informatie is zeer wenselijk bij privacy logs :

[1] Bijv. de KSZ bepaalt dat privacy logs minstens 10 jaar bewaard dienen te worden.

- Het waarom? (Detail van de activiteit / finaliteit)
- De end-of-life datum van de log (Retention time)
- Welke transactie aan de hand van uniek nummer? (Wat) (Transaction ID)

Manuele logboeken

Speciale aandacht zou moeten besteed worden aan manuele logboeken omdat het risico op schending van vertrouwelijkheid, integriteit en beschikbaarheid groter is dan bij geautomatiseerde logging:

- Door de manuele procedure en opvolging is het risico op fouten, inconsistenties, ontbreken van informatie groter;
- Fysieke toegang tot het logboek moet beveiligd worden;
- Beschikbaarheid van het logboek moet gegarandeerd worden, bv. door het nemen van kopieën.

Mitigerende maatregelen om manuele logboeken te beveiligen bestaan o.a. uit:

- Fysieke toegangsbeveiliging d.m.v. afsluitbare/brandveilige kast;
- Kopieën bijhouden van het logboek;
- Inscannen en opslaan als pdf bestand;
- Controle en 4-ogen principe

Retentie en beveiliging van audit records

Audit records dienen best op een beveiligde manier opgeslagen te worden en daarna bijgehouden worden om analyse toe te laten. Dit houdt het volgende in:

- Toepassing van een lifecycle model op de log data, rekening houdend met de operationele beschikbaarheid en de archivering van log data.
- Enkel geautoriseerde personen mogen toegang hebben tot de audit records en log bestanden.
- De parameters van het audit systeem mogen enkel gewijzigd worden door geautoriseerd personeel en met toepassing van het 4-ogen principe.
- Audit records moeten beschikbaar zijn voor analyse en rapportering wanneer nodig, b.v. in geval van een intern of extern onderzoek.
- Audit records moeten voldoende lang bijgehouden worden, in lijn met de toepasbare wet- en regelgeving.

Opslag management

Zoals hierboven beschreven dienen audit records voldoende lang bijgehouden worden. Dit betekent ook dat voldoende opslagcapaciteit – eventueel offline – beschikbaar moet zijn en dat er rekening moet worden gehouden met potentiële impact op performantie van het systeem/de toepassing.

Ook voor logging moet het principe van dataminimalisatie worden toegepast. Don’t log what you don’t need!

Omgaan met fouten in auditing

Om te garanderen dat audit informatie steeds voorhanden is, is het belangrijk dat fouten tijdens de logging tijdig worden opgespoord en verholpen worden. Daarom zou logging zodanig opgezet moeten worden dat geautoriseerd personeel automatisch op de hoogte wordt gebracht van problemen. Dit kan gaan over problemen met betrekking tot het aanmaken en beheren van log informatie.

Als er niet meer gelogd kan worden, kan niet meer worden aangetoond wie toegang heeft gehad tot een systeem of tot informatie, of berichten ontvangen of verzonden zijn, of dat gegevens zijn ingevoerd en door wie. Dit brengt risico's voor de informatieveiligheid met zich mee.

De federale organisaties zullen de volgende keuzes maken:

- Het systeem of de toepassing normaal te laten functioneren en geen logging opslaan met als gevolg dat de log informatie verloren gaat.
- Het systeem of de toepassing lokaal te laten loggen en later de logging te synchroniseren. Veel systemen/toepassingen kunnen lokaal loggen, waardoor de log informatie tijdelijk wordt veilig gesteld. Op het moment dat het centrale logmechanisme weer beschikbaar komt, worden de verzamelde records alsnog doorgestuurd. Er moet wel over gewaakt worden dat de lokale logging niet alle beschikbare opslagcapaciteit van het systeem verbruikt. Op het moment dat de lokale opslag volloopt, moet opnieuw besloten worden of men in productie blijft of niet.
- Het systeem of de toepassing uit productie te nemen. Dit betekent dat de daaraan gekoppelde businessprocessen als dusdanig niet meer beschikbaar zijn, en het business continuity proces mogelijk moet worden geactiveerd. Het uit productie nemen betekent dat inbreuken niet ongemerkt kunnen plaatsvinden en ook dat de audit log geen hiaten gaat vertonen, maar dit gaat ten koste van de operationele werking.

Audit opvolging, analyse en rapportering

Log bestanden moeten regelmatig geanalyseerd worden om:

- Afwijkingen op beleidslijnen te detecteren,
- Ongewone activiteiten op te sporen en op te volgen,
- De effectiviteit van veiligheidsmaatregelen te testen.

Audit rapporten moeten periodisch aangemaakt worden en ter beschikking gesteld worden aan het management. Men moet voorkomen dat de rapportering enkel uit technische details bestaat.

Audit rapportering moet worden geïntegreerd in het proces voor incident- en probleem beheer. Enkel geautoriseerd personeel mag audit rapporten aanmaken en reviewen.

Link met andere maatregelen

Link met PAM als maatregel

De maatregel PAM of Privileged Access Management beschrijft hoe het gebruik van geprivilegieerde rechten zoals toegekend aan systeembeheerders, ontwikkelaars,… moet worden toegekend en opgevolgd. Dit wordt beschreven in het document 'IAM + PAM'.

Link met cryptografische maatregelen

Log bestanden bevatten een groot scala aan informatie en moeten dus op hun beurt voldoen aan het informatieclassificatie model. Als gevolg daarvan is het denkbaar dat log informatie de informatiecategorie 3 of hoger toegekend krijgt, of dat er persoonsgegevens in de logbestanden opgeslagen worden, waardoor de maatregelen rond cryptografie zoals beschreven in het document 'Cryptografie beleid', van toepassing zijn.

Documentbeheer

Historiek

Datum	*Auteur*	*Versie*	*Omschrijving wijzigingen*
13/06/2019	BOSA	V0.1	Eerste ontwerp
18/06/2019	FISP workgroup	V1.0	Update op basis van commentaar
20/06/2019	FISP workgroup	V1.1	Update op basis van opmerkingen van de WG-vergadering
21/11/2019	FISP workgroup	V1.2	Publieke verspreiding

Goedkeuringen

Datum	*Approver(s)*	*Versie*
21/11/2019	FISP workgroup	V.1.2

Bronnen

Dit document werd samengesteld met behulp van de volgende bronnen:

- Vo Informatieclassificatie – Minimale maatregelen – SIEM
- KSZ – BLD LOG
- IEC 27001/2

Link met een ander beleid

Afhankelijkheid van interne documenten

Ref	*Titel*
FISPDOC01	*Handleiding voor informatiecategorisatie*

Positionering van het beleid t.o.v. de ISO 27001-norm

Sectie	***Doelstellingen en referentiemaatregelen***	*In relatie (X = Ja*
	Context van de organisatie	
	Leiderschap	
	Planning	
	Ondersteuning	
	Operatie	
	Evaluatie van de prestaties	
	Verbeteringen	

Positionering van het beleid t.o.v. de ISO 27002-norm

Sectie	**Doelstellingen en referentiemaatregelen**	In Relatie *(X = Ja)*	Doelstellingen / Maatregelen *(Detail)*
	Informatiebeveiligingsbeleid		
	Organisatie van informatiebeveiliging		
	Human Resources Veiligheid		
	Asset Management		
	Toegangscontrole		
	Geheimschrift		
	Fysieke en ecologische veiligheid		
	Operationele veiligheid	*x*	*12.4*
	Beveiliging van communicatie		
	Aankoop, ontwikkeling en onderhoud van informatiesystemen		
	Relaties met leveranciers		
	Beheer van informatiebeveiligingsincidenten		
	Informatiebeveiliging in Business Continuity Management		
	Conformiteit		