# Beleidslijn informatieveiligheid en privacy

# Incidentenbeheer

## (BLD INCID)

# INHOUDSOPGAVE

# 1. Inleiding

Dit document maakt integraal deel uit van de methodologie informatieveiligheid en privacy binnen de sociale zekerheid. Dit document is bestemd voor de verantwoordelijken, voor de verwerkers van informatie, voor de informatieveiligheidsconsulent (CISO) en voor de functionaris voor de gegevensbescherming (DPO) van de openbare instelling van de sociale zekerheid (OISZ).

Incidentenbeheer hoort samen met het informatieveiligheidsbeleid, risicobeheer en continuïteitsbeheer tot de belangrijkste aandachtsgebieden van de beleidslijnen. Incidentenbeheer is belangrijk omdat absolute informatieveiligheid en absolute privacy niet bestaan en omdat incidenten niet te voorkomen zijn. Het is niet de vraag óf er iets gaat gebeuren maar wanneer. De belangrijkste te verwachte incidenten kunnen van te voren bedacht worden en de bijpassende reactie en escalatie procedure kan dus ook van te voren uitgewerkt en geoefend worden.

Het incidentenbeheer van de organisatie geeft richting aan de wijze waarop de organisatie wenst om te gaan met alle incidenten en “bijna incidenten” op het gebied van informatieveiligheid en privacy. De organisatie onderschrijft het belang van een adequate behandeling van incidenten en de reactie daarop om daarmee de gevolgen op de werking van de organisatie te minimaliseren. Incidenten dienen gestructureerd te worden behandeld en er moeten procedures worden vastgesteld om de reactie op incidenten doeltreffend en ordelijk te laten plaatsvinden. De organisatie wil leren van incidenten, en daarom moeten incidenten geëvalueerd worden.

Incidentenbeheer op het gebied van informatieveiligheid en privacy omvatten de monitoring en detectie van veiligheidsincidenten op informatie en informatiesysteem (“security incidents”) en van privacy-incidenten (“data breaches”), maar ook het waarnemen van verdachte activiteiten door de medewerkers van de organisatie en de uitvoering van de juiste antwoorden op deze gebeurtenissen.

Incidentenbeheer is het proces van het beheer en de bescherming van informatiesystemen en de daarin opgeslagen informatie. Organisaties moeten zich bewustzijn van hun verantwoordelijkheden als het gaat om de bescherming van deze informatie ten behoeve van de burgers en andere organisaties. Deze verantwoordelijkheid strekt zich uit tot het hebben van een draaiboek voor “wat te doen, als er iets misgaat”. Incidentenbeheer is een set van activiteiten die een proces definieert en implementeert, die een organisatie kan gebruiken om zijn eigen welzijn en de veiligheid van het publiek te bevorderen.

# 2. Beheer van incidenten

Elke organisatie onderschrijft de volgende beleidslijnen van informatieveiligheid en privacy voor alle informatie en informatiesystemen onder de verantwoordelijkheid van de organisatie:

1. Er zijn procedures voor het vastleggen en beheren van incidenten over informatieveiligheid of privacy en de bijhorende verantwoordelijkheden. Deze procedures moeten bekend zijn bij alle medewerkers.
2. Elke medewerker (zowel vast of tijdelijk, intern of extern) is verplicht melding te maken van ongeautoriseerde toegang, gebruik, verandering, openbaring, verlies of vernietiging van informatie en informatiesystemen.
3. Gebeurtenissen en zwakheden over informatieveiligheid of privacy die verband houden met informatie en informatiesystemen van de organisatie worden zodanig kenbaar gemaakt dat de organisatie tijdig en adequaat corrigerende maatregelen kan nemen.
4. Incidenten over informatieveiligheid en privacy moeten zo snel als mogelijk via de leidinggevende, de helpdesk, de informatieveiligheidsconsulent (CISO) of functionaris van gegevensbescherming (DPO) gerapporteerd worden.
5. Incidenten over informatieveiligheid of privacy vereisen het correct verzamelen van bewijsmateriaal in overeenstemming met wettelijke en regelgevende voorschriften.
6. Elk incident over informatieveiligheid of privacy moet formeel geëvalueerd worden opdat procedures en controlemaatregelen verbeterd kunnen worden. De lessen die getrokken worden uit een incident dienen gecommuniceerd te worden naar de directie van de organisatie voor validatie en goedkeuring van verdere acties.

# Bijlage A: Documentbeheer

Versiebeheer

| Datum | Auteur | Versie | Beschrijving van de verandering | Datum goedkeuring | Datum in werking treden |
|---|---|---|---|---|---|
| 2007 | | V2007 | Eerste versie | 10/10/2007 | 10/10/2007 |
| 2017 | | V2017 | Integratie EU GDPR | 07/03/2017 | 07/03/2017 |
| | | | | | |
| | | | | | |

Fouten en weglatingen

Wanneer bij het lezen van dit document fouten of problemen worden vastgesteld, dan wordt u als lezer verzocht om een korte beschrijving van de fout of het probleem en de locatie in het document samen uw contactinformatie door te geven aan de informatieveiligheidsconsulent (CISO) / functionaris van gegevensbescherming (DPO) van de organisatie.

Definities

Om consistentie te garanderen in gebruikte terminologie en begrippen doorheen alle beleidsdocumenten, worden alle definities met betrekking tot informatieveiligheid en privacy gecentraliseerd in één document genaamd “Definities informatieveiligheid en privacy”.

# Bijlage B: Referenties

Hieronder staan documenten vermeld die hebben gediend als inspiratie voor dit document:


- ISO, “ISO/IEC 27001:2013 Information Security Management System Requirements”, september 2013, 23 blz.
- ISO, “ISO/IEC 27002:2013 Code of Practice for Information Security Management”, september 2013, 80 blz.
- ISO, “ISO/IEC 27035:2016 part 1 Information security incident management -- Part 1: Principles of incident management”, november 2016, 21 blz.
- ISO, “ISO/IEC 27035:2016 part 2 Information security incident management -- Part 2: Guidelines to plan and prepare for incident response”, november 2016, 57 blz.
- ISACA, “COBIT 5 for Information Security”, Mei 2012, 220 blz.
- CCB, “Gids voor incidentbeheer”, februari 2016, 38 blz.
- NIST, “Computer Security Incident Handling Guide”, Augustus 2012, 70 blz.


Hieronder staan referenties naar websites die hebben gediend als inspiratie voor dit document:


- https://www.iso.org/isoiec-27001-information-security.html
- http://www.iso.org/iso/catalogue_detail?csnumber=54534
- https://www.iso.org/standard/60803.html
- https://www.iso.org/standard/62071.html
- http://www.isaca.org/cobit
- https://wiki.en.it-processmaps.com/index.php/Incident_Management
- http://www.ccb.belgium.be/sites/default/files/documents/CSIMG_2016_NL.pdf
- https://www.cybersimpel.be/nl

# Bijlage C: Richtlijnen rond incidentenbeheer

## Verantwoordelijkheid en procedures opstellen

Doelstelling: Verantwoordelijkheden en procedures pro-actief opstellen om op een snelle, effectieve en geordende manier een antwoord te bieden aan incidenten van informatieveiligheid en privacy.

Richtlijnen

Er moeten verantwoordelijkheden vastgesteld en procedures opgesteld worden, die binnen de organisatie duidelijk gecommuniceerd moeten worden. De volgende onderwerpen moeten behandeld worden:

a) Hoe omgaan met incident (identificeren, indijken, elimineren en herstellen en post-incident activiteiten)

b) Monitoren, detecteren, analyseren en rapporteren van gebeurtenissen en incidenten

c) Loggen van incidenten

d) Hoe omgaan met forensisch bewijsmateriaal

e) Evalueren van en beslissen over gebeurtenissen en welke beslissingen nemen

f) Hoe kwetsbaarheden op vlak van informatieveiligheid en/of privacy evalueren

g) Escaleren van incidenten

h) Hoe vanaf incidenten een normale situatie herstellen

i) Wat, hoe en wie communiceren naar medewerkers van de organisatie en andere belanghebbenden.

Rapportering van incidenten moet op een gestandaardiseerde manier verlopen, om te verzekeren dat het efficiënt en effectief gebeurt.

Voor niet geautomatiseerde meldingen van gebeurtenissen moeten volgende vragen beantwoord worden:

j) Wat was de gebeurtenis

k) Wie heeft de feiten vastgesteld

l) Wanneer heeft de gebeurtenis plaatsgevonden

m) Wanneer werden de feiten vastgesteld

n) Hoe werd de gebeurtenis veroorzaakt

o) Hoe werden de feiten vastgesteld

p) Wat heeft de gebeurtenis beïnvloed

q) De (potentiele) impact van de gebeurtenis op de activiteiten van de organisatie.

Voor geautomatiseerde meldingen, zie de beleidslijnen “Logging”.

## Zwakheden rapporteren

Doelstelling: werknemers en derde partijen die informatiesystemen en -diensten van de organisatie gebruiken moeten elke geobserveerde of veronderstelde zwakheid in informatiesystemen of diensten direct rapporteren.

Richtlijnen

- Wanneer interne of externe medewerkers van de organisatie zwakheden vermoeden of detecteren moeten zij die zo snel mogelijk melden.
- Het meldingsproces moet eenvoudig, toegankelijk en beschikbaar zijn voor iedereen.

- Gebruikers moeten weten dat ze onder geen beding mogen proberen om zwakheden in informatieveiligheid of privacy uit te buiten.

## Gebeurtenissen identificeren en rapporteren

Doelstelling: gebeurtenissen zo snel mogelijk via de geëigende kanalen identificeren en rapporteren.

Richtlijnen

Heeft een incident zich daadwerkelijk plaatsgevonden, is er wel een inbreuk op de informatieveiligheid of privacy? Deze activiteit omvat normaliter de systeembeheerder en eindgebruiker, maar kan ook het gevolg zijn van pro-actieve detectie van incidenten door de ICT-veiligheid of het systeembeheer of doordat bij de controle van de logging iets naar boven komt. Indien wordt vastgesteld dat het inderdaad een incident is, dan moeten de relevante partijen gewaarschuwd worden.

- Alle medewerkers van de organisatie moeten op de hoogte worden gebracht van hun verantwoordelijkheid om vermoedelijke gebeurtenissen rond informatieveiligheid of privacy zo snel mogelijk te melden bij een centraal meldpunt. Daarnaast moeten zij op de hoogte zijn van de procedure voor het melden van dergelijke gebeurtenissen.
- Voor de volgende situaties (niet exhaustieve lijst) moet overwogen worden of een melding gemaakt moet worden:
    - Ineffectieve veiligheidscontrole
    - Inbreuk op integriteit, betrouwbaarheid of beschikbaarheid van informatie
    - Menselijke fouten met betrekking tot informatie veiligheid
    - Niet-naleving van procedures of richtlijnen met betrekking tot informatieveiligheid
    - Inbreuk op fysieke beveiliging
    - Inbreuk op de privacy
    - Niet gecontroleerde veranderingen aan systemen
    - Verkeerde werking van software of hardware
    - Inbreuken op het toegangsbeleid.
- Er moet feedback gegeven worden over de ondernomen acties aan de bevoegde instantie(s). In functie van de gevolgen van ondernomen acties kan de persoon die de gebeurtenis gemeld heeft door de bevoegde instantie(s) eveneens op de hoogte gebracht worden.

## Beoordeling van / beslissen over gebeurtenissen

Doelstelling: Gebeurtenissen beoordelen en beslissen of deze als incident dienen gekwalificeerd te worden

Richtlijnen

De manager van de afdeling waar een incident optreedt, wijst een incident reactie-leider aan en deze stelt een bij het incident passend incident-team samen. De manager informeert en vraagt zo nodig hulp aan de informatieveiligheidsconsulent (CISO) of functionaris van gegevensbescherming (DPO). Bij een datalek met persoonsgegevens wordt altijd de functionaris van gegevensbescherming (DPO) geïnformeerd en ook de informatieveiligheidsconsulent (CISO). Bij grote incidenten zal de informatieveiligheidsconsulent (CISO) in de meeste gevallen de teamleider worden. Dit team is belast met het beperken van verdere schade als gevolg van het incident. Een grondige beoordeling van de aard en omvang van het incident wordt uitgevoerd tesamen met de schade is en bewijsmateriaal wordt veilig gesteld. Bij een datalek dient de informatie door te stromen naar de privacy commissie binnen de 72 uur na vaststelling.

- Er moeten criteria opgesteld worden voor een uniforme classificatieschaal van incidenten rond informatieveiligheid en privacy.
- Het meldpunt voor gebeurtenissen moet een uniforme classificatieschaal gebruiken om te beoordelen of de gebeurtenis als gebeurtenis of als incident beschouwd moet worden.
- De beoordeling en beslissing voor gebeurtenissen mag door het meldpunt doorgegeven worden aan de informatieveiligheidsconsulent (CISO) of de functionaris van gegevensbescherming (DPO) die de beoordeling en beslissing moet bevestigen of opnieuw beoordelen.
- De resultaten van beoordelingen en beslissingen moeten in voldoende detail geregistreerd worden zodat deze bij toekomstige gebeurtenissen/incidenten als referentie of ter verificatie kunnen dienen.

## Verzamelen en veilig stellen van bewijsmateriaal

Doelstelling: procedures definiëren om informatie van incidenten (die als bewijsmateriaal kan dienen in het kader van een forensisch onderzoek) te identificeren, te verzamelen en intact te houden.

Richtlijnen

- Er moeten procedures opgesteld die beschrijven hoe omgegaan moet worden met bewijsmateriaal met het oog op disciplinaire en/of legale acties.
- Deze procedures moeten beschrijven hoe het identificeren, verzamelen en bewaren van bewijsmateriaal moet gebeuren, rekening houdende met de verschillende mediatypes.
- De procedures voor het omgaan met bewijsmateriaal moeten rekening houden met:
    - Keten van bewijsmateriaal
    - Beveiliging van het bewijsmateriaal
    - Beveiliging van de medewerkers van de organisatie, bezoekers of burgers
    - Rollen en verantwoordelijkheden van de betrokken medewerkers, bezoekers of burgers
    - Competentie van medewerkers van de organisatie
    - Documentatie en registratie
    - Rapportering
- Certificatie of andere methoden moeten aangewend worden om gekwalificeerd personeel of geschiktheid van tools te verzekeren, zodat de waarde van het bewijsmateriaal versterkt wordt.
- Indien het verzamelen van forensisch bewijsmateriaal organisatorische en/of juridische grenzen overschrijdt, dan moet nagegaan worden of de organisatie gemachtigd is om de nodige informatie als forensisch bewijsmateriaal te mogen verzamelen.

## Reageren op en herstellen van incidenten

Doelstelling: antwoorden op en herstellen van incidenten in overeenstemming met de relevante procedures.

Richtlijnen

Maatregelen moeten genomen worden om de oorzaak van het incident te blokkeren of te verwijderen, de impact te verminderen door verdere blootstelling van de gevoelige gegevens te voorkomen, de processen herstarten als deze gestopt waren als gevolg van het incident en ervoor zorgen dat risico's die verband houden met dit incident worden verminderd.

- Incidenten moeten behandeld via één centraal contactpunt.
- Bewijsmateriaal moet zo snel mogelijk aansluitend aan het incident verzameld worden.

- Indien nodig moet een forensische analyse uitgevoerd worden.
- Indien nodig moet er geëscaleerd worden.
- Ondernomen acties moeten geregistreerd worden.
- Medewerkers van de organisatie en derde partijen moeten, op een 'need-to-know' basis, op de hoogte gebracht worden van een incident.
- Een post-incident analyse moet gemaakt worden om de oorzaak van het incident te achterhalen.
- De zwakheden die het incident hebben veroorzaakt of hebben bijgedragen tot het incident moeten geanalyseerd en verholpen worden.
- Een incident dat succesvol afgehandeld is, moet formeel afgerond en gerapporteerd worden.
- Elke reactie op incidenten moet leiden tot het herstel van een normale werking, en tot het initiëren van de noodzakelijke herstelprocedures.
- Er moet één centraal incidentenbeheersysteem (tool) gebruik worden waarin alle informatie omtrent gebeurtenissen en –incidenten opgeslagen wordt.
- Naast het tijdstip en datum van het informatie veiligheidsincident wordt ook gedocumenteerd:
    - Wat was waargenomen en welke acties zijn ondernomen (ook gebruik van automatische tools) en waarom
    - De locatie van het bewijsmateriaal
    - Indien van toepassing, hoe en waar werd het bewijsmateriaal bewaard
    - Indien van toepassing, hoe is het bewijsmateriaal geverifieerd geweest
    - Een overzicht van het bewijsmateriaal.

## Leren uit incidenten via rapport en evaluatie

Doelstelling: Kennis uit het analyseren en oplossen van incidenten gebruiken om de waarschijnlijkheid of de impact van toekomstige incidenten te verminderen

Richtlijnen

Identificeer de lessen uit het incident en bespreek deze met het team, rapporteer over het incident, de genomen maatregelen en het verslag, rapporteer indien nodig intern en extern, pas het gevolgde draaiboek aan.

- Er moeten processen en tools beschikbaar zijn om het type, het volume aan en de kost van incidenten te kwantificeren en monitoren.
- De verzamelde informatie over incidenten moet gebruikt worden om terugkerende incidenten met hoge impact te identificeren.
- De evaluatie van incidenten moet gebruikt worden om na te gaan of de huidige controles adequaat zijn. Indien nodig, dan moeten de controles aangepast worden.

## Meldingen bij privacy incidenten

Doelstelling: incidenten rond persoonsgegevens dienen binnen de 72 uur gemeld te worden aan de privacy commissie

Richtlijnen

Indien een incident in verband met persoonsgegevens heeft plaatsgevonden, meldt de verwerkingsverantwoordelijke deze zonder onredelijke vertraging en, indien mogelijk, uiterlijk 72 uur nadat hij er kennis van heeft genomen aan de privacy commissie, tenzij het niet waarschijnlijk is dat de incident in verband

met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van personen. Indien de melding aan de toezichthoudende autoriteit niet binnen 72 uur plaatsvindt, gaat zij vergezeld van een motivering voor de vertraging.

De verwerker informeert de verwerkingsverantwoordelijke zonder onredelijke vertraging zodra hij kennis heeft genomen van een inbreuk in verband met persoonsgegevens:

a) de aard van het incident in verband met persoonsgegevens, waar mogelijk onder vermelding van de categorieën van betrokkenen en persoonsgegevensregisters in kwestie en, bij benadering, het aantal betrokkenen en persoonsgegevensregisters in kwestie;

b) de naam en de contactgegevens van de functionaris voor gegevensbescherming (DPO) of een ander contactpunt waar meer informatie kan worden verkregen;

c) de waarschijnlijke gevolgen van het incident in verband met persoonsgegevens;

d) de maatregelen die de verwerkingsverantwoordelijke heeft voorgesteld of genomen om het incident in verband met persoonsgegevens aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan.

Indien en voor zover het niet mogelijk is om alle informatie gelijktijdig te verstrekken, kan de informatie zonder onredelijke vertraging in stappen worden verstrekt. De verwerkingsverantwoordelijke documenteert alle incidenten in verband met persoonsgegevens, met inbegrip van de feiten omtrent het incident in verband met persoonsgegevens, de gevolgen daarvan en de genomen corrigerende maatregelen. Die documentatie stelt de privacy commissie in staat de naleving te controleren.

Wanneer de inbreuk in verband met persoonsgegevens waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van personen, deelt de verwerkingsverantwoordelijke betrokkene het incident in verband met persoonsgegevens onverwijld mee via een omschrijving, in duidelijke en eenvoudige taal:

a) De aard van het incident

b) De instanties waar meer informatie over het incident kan worden verkregen

c) De aanbevolen maatregelen om de negatieve gevolgen van het incident te beperken

De mededeling aan de betrokkene is niet vereist wanneer een van de volgende voorwaarden is vervuld:

a) de verwerkingsverantwoordelijke heeft passende technische en organisatorische beschermingsmaatregelen genomen en deze maatregelen zijn toegepast op de persoonsgegevens waarop het incident in verband met persoonsgegevens betrekking heeft, met name die welke de persoonsgegevens onbegrijpelijk maken voor onbevoegden, zoals versleuteling;

b) de verwerkingsverantwoordelijke heeft achteraf maatregelen genomen om ervoor te zorgen dat het hoge risico voor de rechten en vrijheden van betrokkenen zich waarschijnlijk niet meer zal voordoen;

c) de mededeling zou onevenredige inspanningen vergen.

In dat geval komt er in de plaats daarvan een openbare mededeling of een soortgelijke maatregel waarbij betrokkenen even doeltreffend worden geïnformeerd.

De privacy commissie kan, na beraad over de kans dat het incident in verband met persoonsgegevens een hoog risico met zich meebrengt, de verwerkingsverantwoordelijke verplichten tot communicatie.

# Bijlage D: Link met de ISO-norm 27002:2013

Hier wijzen we op de voornaamste clausule(s) van de ISO-norm 27002:2013 die verband houden met het onderwerp van het huidige document.

| ISO-norm 27002:2013 | |
|---|---|
| **Veiligheidsbeleid** | |
| **Organisatie van de informatieveiligheid** | |
| **Veilig personeel** | |
| **Beheer van bedrijfsmiddelen** | |
| **Toegangsbeveiliging** | |
| **Cryptografie** | |
| **Fysieke beveiliging en beveiliging van de omgeving** | |
| **Beveiliging processen** | |
| **Communicatieveiligheid** | |
| **Aankopen, onderhouden en ontwikkelen van informatiesystemen** | |
| **Leveranciersrelaties** | |
| **Beheer van veiligheidsincidenten** | **Ja** |
| **Informatieveiligheidsaspecten van continuïteitsbeheer** | |
| **Naleving** | |

***** EINDE VAN DIT DOCUMENT *****