Beleidslijn informatieveiligheid en privacy

Naleving

(BLD COMPLY)

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).

Dit document beschrijft de beleidslijnen met betrekking tot de naleving van wettelijke, reglementaire, statutaire en contractuele vereisten van informatieveiligheid en privacy. Bovendien beschrijft dit document de beleidslijnen met betrekking tot het verifiëren of de implementatie van informatieveiligheid en privacy in overeenstemming is met de verwachtingen van de directie van de organisatie.

2. Naleving

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

1. De organisatie moet periodiek een conformiteitsaudit uitvoeren met betrekking tot de situatie rond informatieveiligheid en privacy zoals beschreven in de beleidslijnen[1].
2. De organisatie moet schending voorkomen van enige wetgeving, wettelijke, regelgevende, statutaire of contractuele verplichtingen gerelateerd aan informatieveiligheid en privacy.
3. De organisatie moet zeker stellen dat informatieveiligheid en privacy geïmplementeerd en operationeel in overeenstemming is met de verwachtingen van de directie.
4. De organisatie moet een formeel disciplinair proces hebben voor werknemers die inbreuk op de informatieveiligheid of privacy hebben gepleegd.

1 Volgens gangbare goede praktijken zou een dergelijke audit minstens één keer per jaar georganiseerd moeten worden. Daarbij is het niet verboden dat de veiligheidsconsulent van een organisatie een audit uitvoert bij een andere organisatie van hetzelfde netwerk. Als de beheersinstelling van een secundair netwerk geen duidelijk zicht heeft op de informatieveiligheid- of privacy-situatie bij één van haar leden, kan zij aan het Sectoraal Comité vragen om een conformiteitsaudit uit te voeren.

Bijlage A: Documentbeheer

Versiebeheer

Datum	Auteur	Versie	Beschrijving van de verandering	Datum goedkeuring	Datum in werking treden
2003		V2003	Eerste versie	10/09/2003	01/10/2003
2004		V2004	Tweede versie	11/02/2004	01/12/2004
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.
- ISACA, “COBIT 5 for Information Security”, Mei 2012, 220 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
- http://www.iso.org/iso/catalogue_detail?csnumber=54533
- http://www.isaca.org/cobit
- https://www.ksz-bcss.fgov.be/nl
- http://www.ccb.belgium.be/nl/documents
- https://www.safeonweb.be/nl
- https://www.safeinternetbanking.be
- https://www.cybersimpel.be/nl

Bijlage C: Richtlijnen rond naleving

Identificatie van toepasselijke wetgeving, regelgeving, statutaire en contractuele vereisten

- Verantwoordelijkheden en specifieke controles moeten gedefinieerd en gedocumenteerd worden
- De veiligheidsconsulent moet er voor zorgen dat wijzigende trends worden geïntegreerd in de ontwikkeling of aanpassing van beleidslijnen en procedures

Intellectuele eigendomsrechten (Intellectual Property Rights of IPR)

- Software die operationele business toepassingen ondersteunt moet ofwel binnen de organisatie ontwikkeld worden, of aangekocht/gehuurd worden bij een gekende en betrouwbare derde partij (software ontwikkelaar).
- Publiek beschikbare software (ook gekend als shareware en freeware) gebruiken is niet toegestaan tenzij op basis van een evaluatie door de ICT dienst en in overleg met en goedkeuring van de veiligheidsconsulent
- Software van derde partijen, die door de organisatie gebruikt wordt, mag niet gekopieerd worden tenzij expliciet toegestaan in de licentie-overeenkomst én goedkeuring hiervoor wordt gegeven door de directie, of voor continuïteitsredenen
- Door de organisatie ter beschikking gestelde software aan gebruikers mag door deze gebruikers niet gekopieerd worden op een opslagmedium, noch getransfereerd worden naar een andere computer, noch vrijgegeven worden aan partijen extern aan de organisatie zonder expliciete toestemming van de ICT dienst
- Bewustmaking van beleidslijnen ter bescherming van IPR (software, documenten, ontwerprechten, trademarks, patenten en broncode licenties) moet onderhouden worden, en bedrijfsmiddelen waarop IPR rust moet worden geïdentificeerd
- Bewijsmateriaal over “eigenaarschap” van licenties moet bijgehouden worden.
- Controles moeten bestaan om na te gaan of het maximum aantal toegelaten gebruikers zoals gedefinieerd in de licentieovereenkomst wordt gerespecteerd
- Nazicht moet worden doorgevoerd dat uitsluitend geautoriseerde software en licentieproducten wordt gebruikt
- Een beleid moet opgesteld worden voor het beëindigen of transfereren van software aan anderen
- Conformiteit moet bestaan met de algemene verkoopsvoorwaarden voor software en voor informatie verkregen van publieke netwerken
- Tenzij toegelaten door de copyright wetgeving mogen boeken, artikels, rapporten of andere documenten niet geheel noch gedeeltelijk gekopieerd worden

Bescherming van documenten van de organisatie

- Bij bescherming van bedrijfsdocumenten moet rekening gehouden worden met de overeenstemmende classificatie op basis van het classificatieschema van de organisatie
- Documenten moeten gecategoriseerd worden volgens type documenten, zoals boekhouding, transactie logs, audit logs, operationele procedures, elk met bijhorende gegevens over retentieperiode
- Stockeren en behandelen van gegevens moet overeenkomstig de specificaties van de leverancier gebeuren
- Bij bewaren op elektronische media moeten er procedures bestaan om de toegang tot gegevens te verzekeren gedurende de ganse retentieperiode, ondanks gewijzigde technologie
- Een retentieschema moet voor gegevens aangeven wat de retentieperiode is
- Het opslagsysteem moet de identificatie van gegevens en retentieperiodes verzekeren alsook de adequate vernietiging van gegevens op het einde van de retentieperiode
- Richtlijnen moeten bestaan over retentie, stockage, behandeling en vernietiging van gegevens

Bescherming van gegevens en geheimhouding van persoonsgegevens

- Een functionaris van gegevensbescherming (DPO) moet aangesteld worden die leidinggevenden, gebruikers en dienstverleners begeleidt bij hun individuele verantwoordelijkheden en procedures die zij dienen te volgen in het kader van de bescherming van persoonsgebonden gegevens (privacy).
- Technische en organisatorische maatregelen moeten geïmplementeerd worden om persoonsgebonden informatie te beschermen

Voorschriften voor het gebruik van cryptografische beheersmaatregelen

- Juridisch advies moet ingewonnen worden over beperkingen met betrekking tot import of export van hardware en software voor uitvoeren van cryptografische functies en tot het gebruik van encryptie

Onafhankelijke evaluatie van informatieveiligheid en privacy

- Onafhankelijk nazicht door interne audit of een externe gespecialiseerde partij kan gevraagd worden door de directie om de geschiktheid, adequaatheid en effectiviteit van de aanpak van informatieveiligheid en privacy voor de organisatie te verzekeren
- Indien de objectieven voor informatieveiligheid en privacy niet gehaald worden, of conformiteit met het beleidslijnen informatieveiligheid en privacy niet bereikt wordt, dan moeten correctieve acties worden geïmplementeerd

Naleving van informatieveiligheidsbeleid en –procedures

- Leidinggevenden moeten identificeren hoe nazicht van conformiteit met het informatieveiligheidsbeleid binnen hun verantwoordelijkheidsdomein wordt uitgevoerd
- Bij niet-conformiteit in gevolge nazicht moeten leidinggevenden:
    - identificeren wat de oorzaken van niet-conformiteit zijn
    - de noodzaak evalueren voor acties om naleving te verzekeren
    - gepaste correctieve acties implementeren
    - effectiviteit van correctieve acties nagaan en afwijkingen of zwakheden identificeren
    - resultaten van geïmplementeerde correctieve acties registreren.

Nazicht technische conformiteit

- Technische conformiteit moet verzekerd worden met behulp van geautomatiseerde hulpmiddelen die technische rapporten genereren en aansluitend geïnterpreteerd worden door een technisch specialist.
- Intrusietesten of evaluaties van zwakheden in informatiesystemen moeten gepland, gedocumenteerd en uitgevoerd worden door uitsluitend geautoriseerde en competente medewerkers

Disciplinaire maatregelen

- De beleidslijnen informatieveiligheid en privacy moeten ter kennis gebracht worden van het personeel van de organisatie. Het personeel moet gemakkelijk leestoegang tot de beleidslijnen hebben en moet bovendien bewust gemaakt worden over haar verplichtingen op het vlak van informatieveiligheid en privacy.
- De vaststelling dat de beleidslijnen en de bijhorende procedures – die ter kennis gebracht zijn van het personeel - niet gerespecteerd worden, kan leiden tot sancties of zelfs juridische vervolging
- Elke medewerker die gevraagd wordt om een activiteit uit te voeren die in strijd is met dit beleid, moet zo snel mogelijk een schriftelijk of mondeling bezwaar indienen bij de leidinggevende van de dienst, of bij enig ander leidinggevende, of bij de veiligheidsconsulent.

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	
Informatieveiligheidsaspecten van continuïteitsbeheer	
Naleving	**Ja**

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