Beleidslijn informatieveiligheid en privacy

Personeelsgerelateerde aspecten

(BLD HR)

INHOUDSOPGAVE

1. INLEIDING 3
2. PERSONEELSGERELATEERDE ASPECTEN 3
BIJLAGE A: DOCUMENTBEHEER 5
BIJLAGE B: REFERENTIES 5
BIJLAGE C: RICHTLIJNEN ROND PERSONEELSGERELATEERDE ASPECTEN VAN INFORMATIEVEILIGHEID EN PRIVACY ... 6
BIJLAGE D: LINK MET DE ISO-NORM 27002:2013 7

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 beleidslijn 'personeelsgerelateerde aspecten' in samenhang met informatieveiligheid en privacy.

2. Personeelsgerelateerde aspecten

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

Voorafgaand aan het dienstverband: bewerkstelligen dat werknemers, ingehuurd personeel en externe gebruikers hun verantwoordelijkheden begrijpen, geschikt zijn voor de rollen waarvoor zij worden overwogen, en het risico op diefstal, fraude of misbruik van faciliteiten verminderd wordt

- Verificatie van de achtergrond van kandidaten voor functies die een belangrijk risico vormen voor informatieveiligheid, kan uitgevoerd worden overeenkomstig relevante wetten en voorschriften, en moet evenredig zijn met de eisen, de classificatie van de informatie waartoe toegang verleend wordt, en de ingeschatte risico's.
- Als onderdeel van hun contractuele verplichting dienen ingehuurd personeel en externe gebruikers de algemene voorwaarden te aanvaarden en hun arbeidscontract te ondertekenen, waarin hun verantwoordelijkheden en die van de organisatie ten aanzien van informatieveiligheid en privacy moeten vastgelegd zijn.

Tijdens het dienstverband: bewerkstelligen dat alle werknemers, ingehuurd personeel en externe gebruikers zich bewust zijn van bedreigingen en gevaren voor informatieveiligheid, van hun verantwoordelijkheid en aansprakelijkheid. Zij moeten toegerust zijn om het beveiligingsbeleid van de organisatie in de dagelijkse werkzaamheden te ondersteunen, en het risico van een menselijke fout te verminderen

- De directie moet van werknemers, ingehuurd personeel en externe gebruikers eisen dat ze informatieveiligheid en privacy toepassen overeenkomstig de beleidslijnen, minimale normen en procedures van de organisatie
- Alle werknemers van de organisatie en, voor zover van toepassing, ingehuurd personeel en externe gebruikers, moeten geschikte training en regelmatige bijscholing krijgen met betrekking tot beleidslijnen,, minimale normen en procedures van de organisatie, voor zover relevant voor hun rol of functie
- Regelmatig actualiseren van de verificatie van de achtergrond van medewerkers voor functies die een belangrijk risico vormen voor informatieveiligheid en privacy, overeenkomstig relevante wetten en voorschriften, en moet evenredig zijn met de vereisten, de classificatie van de informatie waartoe toegang verleend wordt, en de ingeschatte risico's
- Er moet een formeel disciplinair proces voorzien zijn voor medewerkers die een inbreuk op informatieveiligheid of privacy hebben gepleegd, en dit in overeenstemming met sancties voor niet naleving zoals voorzien in de wetgeving

Beëindiging of wijziging van dienstverband: Bewerkstelligen dat de belangen van de organisatie beschermd worden indien werknemers, ingehuurd personeel en externe gebruikers de organisatie verlaten of hun dienstverband binnen de organisatie wijzigen

- De verantwoordelijkheden en verplichtingen rond informatieveiligheid en privacy die geldig blijven na beëindiging of wijziging van het dienstverband moeten duidelijk zijn vastgesteld, gecommuniceerd worden aan de medewerker, ingehuurd personeel en externe gebruikers, en afgedwongen worden.

Daarnaast moet elke organisatie:

1. een informatieveiligheidsdienst inrichten die wordt geleid door een veiligheidsconsulent, of die taak toevertrouwen aan een erkende gespecialiseerde informatieveiligheidsdienst. De informatieveiligheidsdienst heeft een adviserende, stimulerende, documenterende en controlerende opdracht (in de zin van het KB van 1993). Met het oog op de veiligheid van de sociale gegevens die door de organisatie worden verwerkt en met het oog op de bescherming van de persoonlijke levenssfeer van de personen op wie de sociale gegevens betrekking hebben, staat de veiligheidsconsulent in voor:
    a. het verstrekken van deskundige adviezen aan de persoon belast met het dagelijks bestuur;
    b. het uitvoeren van opdrachten die hem door de persoon belast met het dagelijks bestuur worden toevertrouwd.
2. de identiteit van haar veiligheidsconsulent en zijn eventuele adjuncten meedelen aan het sectoraal comité van de sociale zekerheid en van de gezondheid. Voor de organisaties van het secundaire netwerk moet de identiteit meegedeeld worden aan de organisatie.
3. in het bezit zijn van een veiligheidsplan dat door de verantwoordelijke voor het dagelijkse bestuur van de betrokken organisatie (of gelijkwaardig),werd goedgekeurd.
4. over de nodige werkingskredieten beschikken die door de verantwoordelijke voor het dagelijkse bestuur van de betrokken organisatie (of gelijkwaardig),werden goedgekeurd, teneinde te kunnen voorzien in de uitvoering van haar veiligheidsplan en de uitvoering door de veiligheidsdienst van de haar opgedragen taken.
5. aan de KSZ het aantal uren meedelen dat ze officieel aan de veiligheidsconsulent en aan zijn eventuele adjuncten heeft toegekend voor de uitvoering van hun taken.
6. de communicatie van informatie aan de veiligheidsconsulent zodanig organiseren dat hij over de gegevens beschikt voor de uitvoering van de hem toegewezen veiligheidsopdracht en om overleg te organiseren tussen de verschillende betrokken partijen[1] teneinde op deze manier de veiligheidsconsulent nauwer te betrekken bij de werkzaamheden van de organisatie.

Elke organisatie moet beschikken over een beslissingsplatform voor de validatie en de goedkeuring van de informatieveiligheid- en privacy-maatregelen

Elke organisatie van een secundair netwerk is ertoe gehouden om minstens één keer per semester relevante informatie uit te wisselen met haar secundair netwerk door een vergadering van de subwerkgroep "Informatieveiligheid" te organiseren voor de organisaties die deel uitmaken van haar netwerk

Elke organisatie moet over procedures beschikken voor de ontwikkeling van nieuwe systemen of belangrijke evoluties van bestaande systemen zodat door de projectverantwoordelijke rekening wordt gehouden met de informatieveiligheid- en privacy-vereisten die in dit document beschreven worden

1 De partijen waar in deze beleidslijn naar wordt verwezen zijn voornamelijk de leden van de informaticadienst (ontwikkeling en productie), de preventie-adviseur, de veiligheidsconsulent en de diensten die de gegevens beheren.

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 personeelsgerelateerde aspecten van informatieveiligheid en privacy

Voorafgaand aan het dienstverband

Screening

- De verantwoordelijkheden ten aanzien van informatiebeveiliging moeten vóór het dienstverband worden vastgelegd in passende functiebeschrijvingen en in de arbeidsvoorwaarden
- Kandidaten voor functies die een belangrijk risico vormen voor de informatieveiligheid, in het bijzonder voor vertrouwensfuncties en veiligheidsfuncties, kunnen gescreend worden
- Functies die een belangrijk risico voor de informatieveiligheid vormen moeten door de organisatie geïdentificeerd en gedocumenteerd worden
- Procedures moeten beschrijven op basis van welke criteria verificaties mogen uitgevoerd worden, wie dat mag doen, hoe en wanneer

Arbeidsvoorwaarden

- Ingehuurd personeel en externe gebruikers die ICT-voorzieningen gebruiken moeten een overeenkomst ondertekenen over hun rollen en verantwoordelijkheden met betrekking tot informatieveiligheid
- Het bestek voor een overheidsopdracht moet de kernprincipes bevatten die de opdrachtnemer en zijn personeel moeten respecteren en toepassen tijdens de uitvoering van de opdracht. De kernprincipes informatieveiligheid en privacy zullen tijdens uitvoering vervolledigd en gepreciseerd worden met specifieke richtlijnen. Deze richtlijnen mogen geen afbreuk doen aan de kernprincipes
- Het personeel dat door een leverancier ter beschikking wordt gesteld van de organisatie in het kader van een overheidsopdracht moet zich houden aan de voorwaarden zoals gedefinieerd in het bestek én aan de specifieke richtlijnen gecommuniceerd tijdens uitvoering van de opdracht
- Rollen en verantwoordelijkheden in verband met informatieveiligheid en privacy dienen reeds tijdens het indienstnemingsproces te worden gecommuniceerd aan kandidaat werknemers.

Tijdens het dienstverband

Directieverantwoordelijkheid

- Werknemers, ingehuurd personeel en externe gebruikers moeten gepast ingelicht worden over hun rol en verantwoordelijkheid en de nodige richtlijnen verstrekt worden, alvorens toegang te verlenen tot vertrouwelijke informatie of informatiesystemen van de organisatie.

Bewustmaking, opleiding en training ten aanzien van informatiebeveiliging en privacy

- Een bewustmakingsprogramma rond informatieveiligheid en privacy moet opgesteld worden dat gealigneerd is met de geldende beleidslijnen en procedures van informatieveiligheid en privacy
- Een sensibiliseringsprogramma moet bestaan uit verschillende sensibiliseringsinitiatieven zoals bijvoorbeeld informatiesessies, nieuwsbrieven, posters, enz., en moet geregeld geactualiseerd en georganiseerd te worden
- Opleiding met betrekking tot informatieveiligheid en privacy moet eveneens geregeld georganiseerd worden zowel voor nieuwkomers als voor diegenen die van functie of rol veranderen binnen de organisatie

Actualiseren screening

- Kandidaten voor functies die een belangrijk risico vormen voor de informatieveiligheid en privacy, in het bijzonder voor vertrouwensfuncties en veiligheidsfuncties, kunnen regelmatig gescreend worden

Disciplinaire maatregelen

- De vaststelling dat het beleid en de bijhorende procedures – die ter kennis gebracht zijn van het personeel - niet gerespecteerd worden, kan leiden tot sancties of zelfs juridische vervolging

- Disciplinaire maatregelen voor werknemers van de organisatie moeten in overeenstemming zijn met interne sancties voorzien in de wetgeving
- Sancties voor ingehuurd personeel en contractors, andere dan die reeds voorzien zijn in de algemene wetgeving, of door de wet- en regelgeving inzake overheidsopdrachten, moeten vermeld worden in het bestek

Beëindiging of wijziging van dienstverband

- Verantwoordelijkheden op het vlak van informatieveiligheid en privacy die gedurende een bepaalde periode na beëindiging van het dienstverband nog zouden verder lopen moeten voorafgaandelijk in bijzondere clausules of overeenkomsten voor tewerkstelling opgenomen worden
- Diegene bij de organisatie die verantwoordelijk is voor het toezicht en opvolging van het ingehuurd personeel en externe gebruikers moet de voorgaande richtlijnen toepassen voor ingehuurd personeel en externe gebruikers

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	**Ja**
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	

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