Beleidslijn informatieveiligheid en privacy

Fysieke veiligheid

(BLD PHYS)

INHOUDSOPGAVE

1. Inleiding

Dit document maakt integraal deel uit van de beleidslijnen 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 rond fysieke beveiliging en omgevingsbeveiliging.

2. Veilige fysieke omgeving

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

2.1. Beveiligde ruimten

Elke organisatie moet de toegang tot de gebouwen en lokalen beperken tot de geautoriseerde personen en een controle erop verrichten zowel tijdens als buiten de werkuren.

a. Er moeten toegangsbeveiligingen (barrières zoals muren, toegangspoorten met kaartsloten of een bemande receptie) worden aangebracht om ruimten te beschermen waar zich gevoelige of kritische informatie en ICT voorzieningen bevinden.

b. Privaat toegankelijke zones van een gebouw en de beveiligde ruimten moeten worden beschermd door geschikte toegangsbeveiliging, om te bewerkstelligen dat alleen bevoegd personeel wordt toegelaten.

c. Er moet fysieke beveiliging van kantoren, ruimten en faciliteiten worden ontworpen en gerealiseerd.

d. Elke organisatie moet maatregelen treffen m.b.t. de preventie, de bescherming, de detectie, het blussen en de interventie in geval van brand, inbraak of waterschade.

e. Er moeten fysieke bescherming en richtlijnen voor werken in beveiligde ruimten worden ontworpen en gerealiseerd.

f. Toegangspunten zoals gebieden voor laden en lossen en andere punten waar onbevoegden het terrein kunnen betreden, moeten worden beheerst en indien mogelijk worden afgeschermd van kritieke en/of ICT voorzieningen, om onbevoegde toegang te voorkomen.

2.2. Beveiliging van apparatuur

De organisatie moet maatregelen treffen ter voorkoming van verlies, schade, diefstal of compromitteren van bedrijfsmiddelen en onderbreking van de bedrijfsactiviteiten.

a. Kritische apparatuur moet zo worden geplaatst en beschermd dat risico's van schade en storing van buitenaf en de gelegenheid voor onbevoegde toegang wordt verminderd.

b. Elke organisatie moet over een alternatieve stroomvoorziening beschikken om de verwachte dienstverlening te waarborgen. Kritische apparatuur moet worden beschermd tegen stroomuitval en andere storingen door onderbreking van nutsvoorzieningen.

c. Voedings- en telecommunicatiekabels die voor dataverkeer of ondersteunende informatiediensten worden gebruikt, moeten tegen interceptie of beschadiging worden beschermd.

d. Kritische apparatuur moet op correcte wijze worden onderhouden, zodat deze voortdurend beschikbaar is en in goede staat verkeert.

e. Apparatuur, informatie en programmatuur van de organisatie mogen niet zonder voorafgaande toestemming van de locatie worden meegenomen.

f. Apparatuur buiten de locaties moet worden beveiligd, waarbij rekening wordt gehouden met de diverse risico's van werken buiten het terrein van de organisatie.

g. Elke organisatie moet de nodige maatregelen treffen opdat alle gegevens op opslagmedia gewist of ontoegankelijk gemaakt worden vóór verwijdering of hergebruik.

h. Gebruikers moeten zeker stellen dat onbewaakte apparatuur gepast beschermd wordt.

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
2014		V2014	Vierde versie	30/08/2014	01/09/2014
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 TS 30104:2015 Security Techniques – Physical Security Attacks, Mitigation Techniques and Security Requirements.”, Mei 2015, 30 blz.
- ENISA, “Technical guideline for minimum security measures”, December 2011, 22 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
- https://www.iso.org/standard/56890.html
- http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
- https://resilience.enisa.europa.eu/
- http://www.isaca.org/cobit
- https://www.ksz-bcss.fgov.be/nl

Bijlage C: Richtlijnen rond fysieke veiligheid

Fysieke beveiliging van de omgeving

1. Beveiligingsperimeters van het terrein, het openbaar toegankelijk gedeelte van een gebouw, de privaat toegankelijke zone van een gebouw en de beveiligde ruimten moeten geïdentificeerd en gedefinieerd worden.
2. De sterkte van beveiligingsperimeters van gebouwen, zones in gebouwen en ruimten moet afhankelijk zijn van de beveiligingseisen die - op basis van een risicoanalyse - worden gesteld aan informatiebedrijfsmiddelen (zoals apparatuur, applicaties, data) gebruikt binnen deze gebouwen, zones en ruimten.
3. De gebouwen of locaties waar zich kritieke en/of ICT voorzieningen bevinden moeten fysiek afdoende beveiligd zijn.
4. Een bemande receptie of andere voorzieningen om de fysieke toegang tot kritieke gebouwen of locaties te beheren moet aanwezig zijn.
5. Toegang tot de privaat toegankelijke zone van een gebouw en de beveiligde ruimten moet voorbehouden worden voor geautoriseerde personen.
6. Gebouwen gebruikt door de organisatie moeten op het vlak van nutsvoorzieningen en veiligheid ingericht zijn conform de nationale, regionale en, waar toepasselijk internationale wet- en regelgeving. Het is de beheerder van de gebouwen die hiervoor verantwoordelijk is.
7. Voor kritieke gebouwen, zones en ruimten moeten er anti-inbraaksystemen geïnstalleerd worden conform nationale, regionale en eventueel internationale normen. Onbemande kritieke ruimten moeten te allen tijde van een alarmsysteem voorzien zijn. De beveiligingssystemen moeten op regelmatige basis op effectieve werking getest worden.
8. Kritieke branddeuren moeten voorzien zijn van een alarm. Branddeuren moeten gecontroleerd en getest worden op effectieve werking overeenkomstig nationale, regionale of internationale normen.
9. Alarminstallaties, brandmeldsystemen, rookdetectors en nooduitgangen moeten eveneens op regelmatige basis gecontroleerd worden overeenkomstig nationale, regionale of internationale normen.
10. De locatie van archieven en beveiliging ervan moeten zorgvuldig bepaald worden om het risico op niet geautoriseerde toegang tot, ontvreemding van, of beschadiging door brand of waterschade van opgeslagen informatie te vermijden.

Fysieke toegangsbeveiliging

11. Bezoekers van de organisatie moeten geregistreerd worden, met bovendien aanduiding van datum en tijdstip van aankomst en vertrek.
12. Bezoekers van beveiligde kritieke ruimten moeten expliciete toestemming hebben om deze te betreden. Er mag alleen toegang verleend worden voor bepaalde geautoriseerde doeleinden. De medewerkers moeten informatie over verwachte bezoekers voorafgaandelijk doorgeven aan de receptionisten of bewakers, voor zover aanwezig.
13. Toegang tot beveiligde kritieke ruimten moet worden beheerd en moet beperkt worden tot uitsluitend geautoriseerde personen. In dit geval moeten alle toegangen voor auditdoeleinden geregistreerd worden.
14. Alle interne en externe medewerkers van de organisatie en bezoekers moeten een vorm van identificatie zichtbaar dragen in de privaat toegankelijke zone van een gebouw (kantoren), en in de beveiligde ruimten.
15. Medewerkers van externe ondersteunende diensten moeten alleen geautoriseerde toegang krijgen tot beveiligde ruimten of gevoelige ICT voorzieningen wanneer dit vereist wordt door de organisatie.
16. Toegangsrechten tot beveiligde perimeters moeten regelmatig beoordeeld, geactualiseerd en, indien nodig, ingetrokken worden.

Beveiliging van kantoren, ruimten en faciliteiten

17. Gebouwen, zones in gebouwen, verdiepingen en ruimten moeten geclassificeerd worden in functie van de kritieke functies die er uitgevoerd worden.
18. Kritieke voorzieningen moeten in gebouwen, zones in gebouwen of ruimten dusdanig geplaatst worden dat zij niet toegankelijk zijn voor het publiek.
19. Gebouwen, zones in gebouwen of ruimten waarin informatie verwerkende activiteiten plaatsvinden moeten zo onopvallend mogelijk zijn.
20. Informatie over locaties van gevoelige of kritieke ICT voorzieningen mag niet vrij toegankelijk zijn voor het publiek.
21. In kritieke ruimten moet er gebruik gemaakt worden van aangepaste bewakingsmiddelen, bijvoorbeeld camerabewaking.

Bescherming tegen bedreigingen van buitenaf

22. Gevaarlijke materialen moeten op veilige afstand van de kritieke ruimten worden opgeslagen.
23. Back-upmedia moeten op veilige afstand worden bewaard van de locatie waar de informatie verwerkt wordt, zodat deze niet beschadigd worden door een calamiteit op de verwerkingslocatie.

Werken in beveiligde ruimten

24. Het maken van opnames (film, foto, geluid) in kritieke gebouwen, zones in gebouwen of ruimten moet verboden worden, tenzij mits expliciete toelating van en permanente begeleiding door de organisatie.
25. Alleen medewerkers van de organisatie moeten op een ‘need-to-know’ basis afweten van het bestaan van beveiligde gebouwen, zones in gebouwen of ruimten of van activiteiten in die beveiligde gebouwen, zones in gebouwen of ruimten.

Ruimten voor laden en lossen

26. Toegang tot een laad- en losruimten van buitenaf moet voorbehouden zijn aan geautoriseerde medewerkers met geldige en zichtbare vorm van identificatie.
27. Laad- en losruimten moeten zo ontworpen/ingericht zijn dat goederen kunnen afgeleverd worden zonder dat de leverancier andere delen van het gebouw hoeft te betreden.
28. Waar van toepassing, moeten buitendeuren van een laad- en losruimte afgesloten zijn wanneer de binnendeuren worden geopend.
29. Informatiebedrijfsmiddelen moeten bij aankomst op locatie of bij vertrek op de locatie volgens de procedures voor bedrijfsmiddelenbeheer geregistreerd worden.

Plaatsing en bescherming van apparatuur

30. Opslagvoorzieningen moeten beveiligd worden tegen onbevoegde toegang
31. Er moeten controlemaatregelen aangewend worden om het risico van mogelijke gevaren te minimaliseren, zoals bijvoorbeeld diefstal, brand en vandalisme
32. De organisatie moet richtlijnen opstellen en toepassen ten aanzien van eten, drinken en roken in de datacenters onder beheer van de organisatie
33. Omgevingsvoorwaarden zoals temperatuur en luchtvochtigheid, moeten worden bewaakt om te vermijden dat de werking van informatie-verwerkende voorzieningen en de opslag van informatie negatief beïnvloed wordt

Nutsvoorzieningen

34. Alle nutsinstallaties zoals elektriciteits- en watervoorziening, riolering, verwarming/ventilatie en airconditioning moeten berekend zijn op de systemen die ze ondersteunen
35. Nutsinstallaties moeten regelmatig worden geïnspecteerd en waar nodig getest om hun goede werking te waarborgen en om enig risico op defect of uitval te verminderen
36. Er moet een geschikte elektrische voeding aanwezig zijn die voldoet aan de specificaties van de leverancier van de apparatuur
37. Ter ondersteuning van kritieke processen moet UPS-apparatuur (Uninterruptable Power Supply of UPS) en/of één of meer stroomgeneratoren voorzien worden, die regelmatig gecontroleerd en getest moeten worden op effectieve werking en om te waarborgen dat ze voldoende capaciteit hebben
38. Er moet een toereikende brandstofvoorraad en -toevoer voorzien worden om te waarborgen dat de generator voor een lange tijd kan blijven werken
39. Er moet nagegaan worden of er een alarmsysteem moet worden geïnstalleerd om storingen in de nutsinstallaties te detecteren
40. Noodverlichting moet aangebracht zijn voor het geval zich een totale stroomstoring voordoet
41. Er moeten aangepaste uitrustingen zijn om in noodsituaties snel de stroom te kunnen uitschakelen (bv. noodstop of differentieelschakelaar).
42. De watervoorziening moet stabiel en voldoende zijn (bijv. voor airconditioning, bevochtigingsapparatuur en brandbestrijdingssystemen). Voor koeling van datacenters moet er bovendien een zekere reserve aan water voorzien worden voor noodsituaties
43. Telecommunicatie apparatuur moet op ten minste twee verschillende manieren op de systemen van de telecomleverancier worden aangesloten

Beveiliging van kabels

44. Netwerkkabels moeten beschermd worden tegen ongeautoriseerd aftappen of beschadigen, bijvoorbeeld door ze in mantelbuizen of kabelgoten te leggen en zo min mogelijk door openbare ruimten te laten lopen
45. Er moet gebruik gemaakt worden van degelijk kabelbeheer. Bovendien moeten duidelijk identificeerbare markeringen op kabels en apparatuur aangebracht worden om fouten bij onderhoudswerkzaamheden te voorkomen, zoals bijvoorbeeld het per ongeluk patchen van de verkeerde netwerkkabels. Toegang tot patchpanelen en kabelruimten moet beveiligd worden
46. Er moet een centraal overzicht bijgehouden worden van alle gemaakte patches om de kans op fouten te verminderen. Daarnaast moet er voor gevoelige of kritieke systemen gebruik gemaakt worden van detectievoorzieningen en fysieke inspectie, om ongeautoriseerde apparatuur die mogelijks op de bekabeling wordt aangesloten op te sporen

Onderhoud van apparatuur

47. Apparatuur moet onderhouden worden volgens de door de leverancier aanbevolen voorschriften en service-tijdstippen
48. Reparatie en onderhoud van apparatuur moet alleen uitgevoerd worden door bevoegd onderhoudspersoneel
49. Een centraal overzicht moet bijgehouden worden van alle vermeende of daadwerkelijke storingen en van alle preventieve en corrigerende onderhoudswerkzaamheden
50. Procedures moeten opgesteld worden waarin terug te vinden is welk apparatuur wanneer onderhouden moet worden, wie het onderhoud moet verrichten en of er al dan niet informatie van de apparatuur verwijderd moet worden

Meenemen van informatiebedrijfsmiddelen

51. Tenzij er een algemeen beleid bestaat waarbij iedere medewerker informatiebedrijfsmiddelen buiten de locaties van de organisatie mag meenemen, moet er een centraal overzicht bijgehouden worden van alle personen die geautoriseerd zijn om informatiebedrijfsmiddelen buiten de locaties van de organisatie mee te nemen

Beveiliging van apparatuur buiten het terrein

52. Apparatuur en media mogen buiten het terrein niet onbeheerd achtergelaten worden in openbare ruimten. Draagbare computers moeten tijdens het reizen als handbagage vervoerd worden en moeten zo min mogelijk herkenbaar zijn

53. De instructies van de leverancier ter bescherming van de apparatuur moeten te allen tijde opgevolgd worden

Veilig verwijderen en hergebruiken van apparatuur

54. Apparatuur met gevoelige informatie moet ofwel fysiek vernietigd worden of de informatie moet vernietigd, verwijderd of overschreven worden met technieken die het onmogelijk maken de oorspronkelijke informatie terug te halen

55. Voor beschadigde apparatuur die gevoelige informatie bevat moet een risico-beoordeling gemaakt worden om te bepalen of ze vernietigd, gerepareerd of verwijderd moet worden

Onbewaakte hardware van gebruikers

56. Elke eindgebruiker moet op de hoogte worden gesteld van zijn verantwoordelijkheden op vlak van informatieveiligheid en procedures voor het beschermen van onbewaakte hardware van eindgebruikers

57. Hardware van eindgebruikers die niet actief gebruikt wordt moet beveiligd worden door een automatische screensaver en een wachtwoord, waarbij het opnieuw activeren gebaseerd moet zijn op identificatie en authenticatie van de gebruiker

58. Eindgebruikers moeten:

    - actieve sessies volledig afsluiten of vergrendelen wanneer de apparatuur onbewaakt achtergelaten wordt, of bij beëindiging van hun taken/werkzaamheden
    - Uitloggen uit applicaties of netwerkdiensten wanneer deze niet meer nodig zijn.

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	**Ja**
Beveiliging processen	
Communicatieveiligheid	
Aankopen, onderhouden en ontwikkelen van informatiesystemen	
Leveranciersrelaties	
Beheer van veiligheidsincidenten	
Informatieveiligheidsaspecten van continuïteitsbeheer	
Naleving	

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