Beleidslijn informatieveiligheid en privacy

Draadloze netwerken

(BLD WIREL)

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 rond de informatieveiligheid en privacy bij draadloze netwerken.

2. Veilige draadloze netwerken

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 draadloze netwerken beheren en beheersen om toegang tot en gebruik van het netwerk te beperken, en om de informatie in systemen en toepassingen te beschermen die over draadloze netwerken wordt verstuurd
2. De organisatie moet de richtlijnen naleven die beschreven zijn in bijlage C van de beleidslijn ‘veilige draadloze netwerken’

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.
- ISO, “ISO/IEC 27033:2016 Security techniques - Network security Part 6 securing wireless IP network access”, juni 2016, 26 blz.
- ISACA, “COBIT 5 for Information Security”, Mei 2012, 220 blz.
- ISACA, “Mobile Computing security audit/assurance program”, oktober 2010,23 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/51585.html
- http://www.isaca.org/cobit
- http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-153.pdf
- https://www.enisa.europa.eu/topics/data-protection
- http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Mobile-Computing-Security-Audit-Assurance-Program.aspx
- http://www.cnt-nar.be/CAO-COORD/cao-081.pdf
- https://www.cybersimpel.be/nl

Bijlage C: Richtlijnen rond de informatieveiligheid van draadloze netwerken

Deze richtlijnen moeten toegepast worden op alle draadloze netwerken onder beheer van de organisatie op alle locaties

1. Draadloze netwerken voor intern gebruik geven rechtstreeks toegang tot de interne systemen van de organisatie.
2. Draadloze netwerken voor bezoekers geven enkel toegang tot het internet.
3. Draadloze netwerken voor speciaal gebruik worden enkel opgesteld op basis van een speciaal verzoek, wanneer de twee andere draadloze netwerken ontoereikend zijn.
4. Er moet een proces bestaan voor het up-to-date houden van een overzicht waarin de bestaande en toegestane draadloze netwerken, bijhorende veiligheidsprotocollen en alle bijhorende informatieveiligheidsmaatregelen terug te vinden zijn
5. Het netwerk moet periodiek door de ICT dienst gecontroleerd worden op het bestaan van niet-geautoriseerde draadloze netwerken en op het gebruik van geïmplementeerde informatieveiligheidsprotocollen en –maatregelen
6. Er moeten procedures zijn die toelaten om draadloze netwerken in te richten volgens deze veiligheidsrichtlijnen
7. Voor draadloze netwerken die rechtstreeks toegang verlenen tot interne systemen van de organisatie moet er gebruik gemaakt worden van de meest sterke versleuteling
8. Voor draadloze netwerken die rechtstreeks toegang verlenen tot het interne netwerk van de organisatie moet ‘SSID broadcasting’ gedeactiveerd worden
9. Er mag geen gebruik gemaakt worden van zwakke of kwetsbare encryptie-algoritme
10. Gebruikers van draadloze netwerken voor bezoekers waar geen encryptie op actief is, worden op de hoogte gesteld van bijhorende risico’s.
11. Draadloze netwerken voor bezoekers en draadloze netwerken die rechtstreeks toegang geven tot interne systemen van de organisatie moeten logisch gescheiden zijn
12. Draadloze netwerken voor bezoekers moeten enkel toegang geven tot internet en internetdiensten van de organisatie. Rechtstreekse toegang tot interne systemen van de organisatie is niet toegestaan
13. Authenticatiemethoden voor toegang tot draadloze netwerken (behalve draadloze netwerken voor bezoekers) moet bestaan uit sterke authenticatie
14. Draadloze netwerken moeten gemonitord worden op misbruik en pogingen om niet-geautoriseerde toegang te krijgen

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	**Ja**
Cryptografie	
Fysieke beveiliging en beveiliging van de omgeving	**Ja**
Beveiliging processen	
Communicatieveiligheid	**Ja**
Aankopen, onderhouden en ontwikkelen van informatiesystemen	
Leveranciersrelaties	
Beheer van veiligheidsincidenten	
Informatieveiligheidsaspecten van continuïteitsbeheer	
Naleving	

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