Beleidslijn informatieveiligheid en privacy

Mobiele toestellen

(BLD MOBILE)

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).

Het gebruik van mobiele toestellen voor beroepsdoeleinden is onderworpen aan een reeks controlemaatregelen. Elke organisatie dient de gepaste informatieveiligheid- en privacy-maatregelen te treffen om zich te beschermen tegen de risico's die verbonden zijn met het gebruik van mobiele toestellen zoals:

- Verlies van gevoelige informatie door
  - diefstal of verlies van het mobiele toestel
  - eenvoudige wachtwoorden of cijfercombinaties
  - het ontbreken van toegangscontrole tot het mobiele toestel.
- Niet-intentionele verspreiding van gevoelige informatie
- Aanvallen door kwaadwillige programma's zoals malware, spyware, ransomware, …
- Aanvallen verbonden aan het gebruik van internet of e-mail, zoals phishing
- Aanvallen afkomstig via onveilige draadloze netwerken

De beleidslijn geldt zowel voor de mobiele toestellen die door de organisatie ter beschikking worden gesteld als voor private mobiele toestellen.

2. Veilig gebruik van mobiele toestellen

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

Deze beleidslijn is gekoppeld aan de beleidslijn inzake centraal beheer en inventarisatie van toestellen. Deze beleidslijnen dienen door de organisatie opgesteld, gevalideerd, gecommuniceerd en toegepast te worden naar alle betrokken partijen. Deze beleidslijnen gelden voor alle gebruikers die via mobiele toestellen[1] toegang hebben tot informatie van de organisatie.

a. Elke organisatie moet de gepaste maatregelen nemen opdat de professionele, vertrouwelijke en gevoelige gegevens opgeslagen op mobiele media enkel toegankelijk zijn voor geautoriseerde personen.

b. Elke organisatie moet de gepaste maatregelen treffen, in functie van het toegangsmedium[2], voor de informatieveiligheid van de online-toegang van buiten de organisatie tot de professionele, vertrouwelijke en gevoelige gegevens van de organisatie

c. Het gebruik van privé-toestellen voor beroepsdoeleinden kan enkel onder de volgende voorwaarden:

   1) De gebruiksvoorwaarden dienen vastgelegd te worden op basis van een risico-beoordeling die rekening houdt met de legitieme behoeften (onder andere de gebruikte gegevens) en de gebruiksomstandigheden..

   2) De organisatie heeft voldoende garanties dat de private mobiele toestellen over een gelijkaardig informatieveiligheid- en privacy-niveau beschikken als dat van de mobiele toestellen die door de organisatie ter beschikking worden gesteld.

[1] Onder mobiele toestellen dienen in de eerste plaats smartphones en tablets te worden begrepen die gebruik maken van een mobiel besturingssysteem zoals Google Android, Apple iOS, Microsoft Windows, enz. maar de term "mobiele toestel" slaat ook op netbooks en elk andere toestel dat buiten de organisatie kan worden gebruikt.

2 Toegangsmedium : vb. internet, gehuurde verbinding, privaat netwerk, draadloos.

3) De organisatie waarborgt dat de toegang tot de gegevens van de organisatie via mobiele toestel enkel mogelijk is volgens het volgende principe: "Om de informatieveiligheid en de privacy van de gegevens van de organisatie te waarborgen zal het vereiste niveau steeds evenredig zijn aan de aard en de gevoeligheid van de gegevens"

4) Het private mobiele toestel van de eindgebruiker moet beheerd worden door de organisatie[3]

5) Een gebruikersovereenkomst dient afgesloten te worden tussen de gebruiker en de organisatie met betrekking tot het professioneel gebruik van het mobiele toestel. Door de ondertekening van de gebruikersovereenkomst verklaart de gebruiker zich akkoord met de richtlijnen en wordt hij/zij verantwoordelijk voor het gebruik van het mobiele toestel.

d. Indien de mobiele toestellen zowel voor beroepsdoeleinden als privé-doeleinden kunnen worden gebruikt, dient de eindgebruiker de regels van informatieveiligheid en privacy na te leven die door de organisatie werden opgesteld.

1) De gebruiker dient waakzaam te blijven wanneer hij/zij het mobiele toestel voor privé-doeleinden gebruikt, overeenkomstig deze richtlijnen en de specifieke richtlijnen inzake informatieveiligheid en privacy.

2) Elke gebruiker is als enige verantwoordelijk voor het gebruik van het mobiele toestel. De gebruiker is zich bewust van de risico's die verbonden zijn aan mobiele toestellen - zeker in geval van verbinding met het informatiesysteem van de organisatie - en zal daarom de informatieveiligheidsregels naleven teneinde elk misbruik te voorkomen, alsook verlies of diefstal te voorkomen.

3) In geval van verlies of diefstal verwittigt de gebruiker onmiddellijk de bevoegde dienst binnen de organisatie, ook voor een privaat mobiele toestel dat voor beroepsdoeleinden wordt gebruikt.

e. De organisatie zal de eigen mobiele toestellen duidelijk identificeren, veilig configureren (met de nodige anti-malware software en met software die alle data op het toestel vanop afstand kunnen wissen) en de identificatie bijhouden in een centraal register.

f. De organisatie kan de conformiteit van mobiele toestellen inzake de beleidslijnen informatieveiligheid en privacy controleren (vanop afstand via software of ter plaatse via directe controle), teneinde de risico's tot een aanvaardbaar niveau te beperken in lijn met de verwachtingen van de organisatie. Om het niveau te garanderen dient de organisatie de gepaste controles te implementeren[4]. De organisatie is niet verantwoordelijk voor schade of kosten als gevolg van het verlies of de diefstal van privé gegevens.

g. De organisatie verbindt zich ertoe om de gebruikers regelmatig te sensibiliseren omtrent de goede praktijken inzake gebruik en hun verantwoordelijkheden (zeker in verband met het connecteren tot publieke draadloze netwerken).

h. De organisatie zal steeds de mogelijkheid hebben om de toegang tot de informatie van de organisatie (gegevens of toepassingen aanwezig op het mobiele toestel) direct te blokkeren en de gegevens te wissen.

i. De organisatie verbindt zich ertoe de privacy van de gebruiker te respecteren.

[3] Indien het mobiele toestel een logische scheiding van privé- en professionele omgeving ondersteunt, dan blijft de controle beperkt tot de professionele omgeving.

[4] Steeds op basis van een wederzijds akkoord tussen de organisatie en de gebruiker.

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.
- ISACA, “Mobile computing security audit/assurance program”, oktober 2010, 23 blz.
- ENISA, “Smartphone security development guidelines”, December 2016, 28 blz.
- NIST, “Guidelines for managing the security of mobile devices in the enterprise”, juni 2013, 30 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
- http://ccb.belgium.be/nl/guidelines
- https://www.enisa.europa.eu/publications/smartphone-secure-development-guidelines-2016
- http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf
- https://www.safeonweb.be/nl
- https://www.safeinternetbanking.be
- https://www.cybersimpel.be/nl

Bijlage C: Richtlijnen voor het veilig gebruik van mobiele toestellen

Hierna volgen richtlijnen voor de organisatie om mobiele toestellen veilig in te zetten.

1. Het niveau van informatieveiligheid en privacy vereist voor de mobiele toestellen is afhankelijk van de aard en de gevoeligheid van de gegevens. De tabellen hieronder geven een overzicht van de richtlijnen die toegepast dienen te worden in functie van drie technische modellen in verband met het beheer van mobiele toestellen.

A. Technische beheersmodellen in functie van de classificatie van de gegevens

Data classification	Voorbeeld	Mobiele toestel zonder gecentraliseerd beheer	Mobiele toestel met gecentraliseerd beheer	Mobiele toestel met gescheiden omgevingen (Isolatie [5]/ VDI[6])
Publieke gegevens	Website KSZ, Website RSZ	J	J	J
Interne bedrijfsgegevens	Interne strategie, agenda, contacten, mails	Te bepalen[7]	J	J
Vertrouwelijke bedrijfsgegevens	Boekhoudplan, Continuïteitsplan	N	Te bepalen	J
Persoonsgegevens	Persoonlijk dossier HR	N	Te bepalen	J
Sociale persoonsgegevens	gegevens rijksregister	N	N	J
Medische gegevens	Medische gegevens	N	N	J

B. Veiligheidsmaatregelen in functie van het beheersmodel

Opgelegde implementatie van veiligheidsmaatregelen	Mobiele toestel zonder gecentraliseerd beheer	Mobiele toestel met gecentraliseerd beheer	Mobiele toestel gescheiden omgevingen (Isolatie / VDI)
Sensibilisering en responsabilisering	J	J	J
Systeem voor gebruikersauthenticatie op het toestel	Aanbevolen	J	J
Vergrendeling van het toestel bij inactiviteit	Aanbevolen	J	J
Paswoordbeleid	Aanbevolen	J	J
Automatische blokkering na X verkeerde toegangscodes	N	J	J
Beveiligde communicatie voor toegang tot bedrijfsinformatie	J	J	J
Sterke authenticatie voor toegang tot bedrijfsinformatie	Aanbevolen	J	J
Controle van de aanwezigheid van een actieve antimalware software	Aanbevolen	J	J

[5] Isolatie: oplossing die het mogelijk maakt om strikt gescheiden omgevingen te creëren (professioneel en privé) op een mobiele toestel waarbij uitsluitend het professionele gedeelte onder controle staat van de werkgever

[6] Virtual Device Interface: *thin client* geïnstalleerd op een mobile device die toelaat om via een beveiligde sessie op afstand te werken in een professionele omgeving.

[7] De notie "te bepalen" betekent dat de instelling de gegevensset vaststelt die toegankelijk is op basis van de drie beheermodellen

Opgelegde implementatie van veiligheidsmaatregelen	Mobiele toestel zonder gecentraliseerd beheer	Mobiele toestel met gecentraliseerd beheer	Mobiele toestel gescheiden omgevingen (Isolatie / VDI)
Controle van de laatste update van de antimalware	N	J	J
Controle van het toegestaan niveau van OS	N	J	J
Enkel de installatie van applicaties afkomstig van een betrouwbare bron toestaan	Aanbevolen	Aanbevolen	Aanbevolen / J in de omgeving van de organisatie
Beperking van de connectiviteit bij de toegang tot informatie van de organisatie[8]	Aanbevolen	J	J
Vercijfering van de gegevens op het toestel	Aanbevolen	Aanbevolen	Enkel bij isolatie is vercijfering noodzakelijk
Blokkering op afstand	N	J	J
Verwijdering van de gegevens op afstand	N	J	J, binnen de omgeving van het mobiele toestel die voorbehouden is voor de organisatie
Het IMEI-nummer van het toestel noteren	Aanbevolen	Aanbevolen	Aanbevolen

2. De gebruiker zal de informatieveiligheid- en privacy-instellingen niet wijzigen ook al is dit technisch mogelijk. De gebruiker zal het mobiele toestel niet “rooten” of “jailbreaken”[9].
3. De gebruiker wordt verwittigd als het mobiele toestel niet conform is aan de minimale normen informatieveiligheid en privacy.
4. Als het mobiele toestel niet conform is, wordt de toegang tot de informatie van de organisatie geweigerd.
5. In geval van verlies of diefstal wordt het toestel vergrendeld en, indien mogelijk en nodig, worden de gegevens gewist. Dit kan leiden tot het verlies van persoonlijke gegevens die op het mobiele toestel zijn opgeslagen.

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	**Ja**
Beheer van bedrijfsmiddelen	
Toegangsbeveiliging	
Cryptografie	**Ja**

[8] Internetverbinding is niet toegestaan

[9] Rooten is de term waarmee - doorgaans buiten de normale procedure om - toegang wordt verkregen door de eigenaar van het apparaat tot het volledige beheer van een computer, smartphone, e.d. Veel apparaten maken gebruik van een variant van het besturingssysteem Unix waarin de 'superuser' (beheerder) de naam 'root' heeft. Rooten betekent daar in feite niets meer of minder dan toegang krijgen tot het root-account van het apparaat, waar de fabrikant van dat apparaat dat niet toelaat. Om - doorgaans tegen de bedoeling van de fabrikant in - alsnog toegang te krijgen wordt veelal gebruik gemaakt van beveiligingsfouten in het besturingssysteem. Voor sommige besturingssystemen is de term jailbreak gebruikelijker; de gebruiker is als het ware opgesloten in de gevangenis van het besturingssysteem en breekt daar uit.

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

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