Beleidslijn informatieveiligheid en privacy

Veilig toegangsbeheer van portalen

(BLD PORTAL)

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).

Deze beleidslijn verduidelijken de toegangsmodaliteiten voor personen die aangesteld werden als beheerder of medebeheerder van de toegangsmachtigingen tot het portaal van de sociale zekerheid. Machtigingen verlenen betekent toegang geven tot het geheel of een gedeelte van de informatiesystemen van de organisaties die betrokken zijn bij de ontwikkeling van deze portalen, meer bepaald:

- een user account op het portaal van de sociale zekerheid beheren,
- als beheerder een rol van medebeheerder beheren,
- de toegangen tot de verschillende toepassingen en transacties beheren,
- de toegangen tot de omgevingen beheren.

De functie van beheerder of medebeheerder is een vertrouwensopdracht waarvoor een grote eerlijkheid en een strikte naleving van de verplichtingen van de functie noodzakelijk zijn.

2. Veilig toegangsbeheer van portalen

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

Iedere organisatie die gebruik wenst te maken van de diensten en toepassingen van het portaal van de sociale zekerheid ten behoeve van zijn gebruikers is verplicht om minstens één toegangsbeheerder aan te stellen. De functie van beheerder of medebeheerder van de portalen wordt door de persoon die met het dagelijkse bestuur van de organisatie is belast volgens een vastgestelde procedure toegekend.

De informatieveiligheidsconsulent (CISO) is bij ontstentenis de beheerder van de organisatie; hij/zij is de bevoorrechte tussenpersoon tussen de organisatie en de veiligheidsdienst van de Kruispuntbank van de Sociale Zekerheid (KSZ). Naast de naleving moet de informatieveiligheidsconsulent de medewerkers aanzetten tot het lezen en toepassen van de reglementen over het gebruik van de informatiesystemen van de portalen.

De functie van beheerder of medebeheerder omvat minimaal de volgende elementen:

1. De rol van beheerder of medebeheerder is nominatief en kan niet, zelfs tijdelijk, afgestaan worden aan een derde.
2. De toekenning van de toegangen tot de portalen en de diensten ervan ten behoeve van de gebruikers van de organisatie is een procedure die door de persoon die met het dagelijkse bestuur is belast, vastgesteld en gevalideerd wordt.
3. De toekenning van individuele toegangsrechten aan de gebruikers van de organisatie moet verplicht beperkt worden tot de toepassingen die noodzakelijk zijn voor de uitvoering van hun specifieke taken.
4. De mededeling aan of de wijziging van het user account van de gebruikers verloopt volgens een vastgestelde procedure.
5. Bij de beëindiging van de opdracht van een medewerker als beheerder of medebeheerder moet de erkende informatieveiligheidsconsulent van de organisatie onmiddellijk alle nodige maatregelen treffen om de toegangen van deze medewerker tot deze rol af te schaffen en om op te volgen wie de nieuwe beheerder of medebeheerder wordt. Verder moet de erkende informatieveiligheidsconsulent de veiligheidsdienst van de KSZ formeel op de hoogte te brengen met formele bekrachtiging door de persoon belast met het dagelijkse bestuur van de organisatie.

Bijlage A: Documentbeheer

Versiebeheer

Datum	Auteur	Versie	Beschrijving van de verandering	Datum goedkeuring	Datum in werking treden
2003	JMG	V2003	Eerste versie	12/12/2003	12/12/2003
2004	JMG	V2004	Tweede versie	02/04/2004	02/04/2004
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 29146:2016 Security techniques – A framework for access management”, juni 2016, 35 blz.
- ISO, “ISO/IEC 24760:2011 Security techniques – A framework for identity management”, December 2012, 20 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
- https://www.iso.org/standard/54534.html
- https://www.iso.org/standard/54533.html
- https://www.iso.org/standard/45169.html
- https://www.iso.org/standard/57914.html
- http://www.isaca.org/cobit
- https://www.ksz-bcss.fgov.be/nl
- http://www.ccb.belgium.be/nl
- https://www.safeonweb.be/nl

Bijlage C: 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	**Ja**
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 *****