Beleidslijn informatieveiligheid en privacy

Clean desk en clear desk

(BLD CLEAR)

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).

In dit document worden de verantwoordelijkheden van de medewerker beschreven met betrekking tot het behoud van doeltreffende fysieke controles tot informatie binnen de organisatie. Met andere woorden, hoe moet de medewerker de fysieke informatie of IT middelen die hem ter beschikking worden gesteld op een veilige manier beheren met het oog op een optimale bescherming van de informatie van de organisatie. Welke maatregelen moeten worden genomen met betrekking tot de beveiliging van de werkpost om zich tegen een ongeoorloofde toegang tot de informatie te beschermen.

« Clean desk » is verschillend van « Clear desk »:

- « Clean desk »: het is vereist dat alles op het bureau wordt opgeruimd en op een veilige plaats wordt bewaard. Hierdoor kunnen fysieke bureaus door meerdere medewerkers gedeeld worden ("flexdesk").
- « Clear desk »: het is niet nodig om alles wat op het bureau ligt op te ruimen maar het is wel verplicht om de gevoelige informatie ontoegankelijk te maken voor onbevoegden. Elk gevoelig gegeven mag niet onbewaakt worden achtergelaten op het bureau.

2. Clean desk & Clear desk

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

2.1. Toegang tot de informatie

Elke medewerker speelt een belangrijke rol in het vermijden van ongeoorloofde toegang tot gevoelige informatie. Dit geldt zowel voor de toegangen tot de informatiesystemen en toepassingen als voor de fysieke toegang tot lokalen of tot documenten. De medewerking van alle medewerkers is van essentieel belang voor de informatieveiligheid en de privacy.

Een (logisch of fysiek) toegangssysteem is geïmplementeerd om elke ongeoorloofde toegang tot de organisatie te voorkomen. De toegang wordt beveiligd door een duidelijke toegangsprocedure. De gebruiker kan gevoelige en vertrouwelijke informatie oproepen tijdens de uitvoering van zijn dagelijkse taken en ze op een andere plaats bewaren waar de toegangsprocedure niet werkt of niet van toepassing is.

De gebruiker blijft steeds verantwoordelijk voor de informatie, ongeacht de vorm waarin deze informatie wordt opgeslagen. De gebruiker moet dus zorgen voor een goede bescherming ervan. Zodra de informatie niet meer wordt gebruikt door de gebruiker, moet de gebruiker zorgen voor de archivering of verwijdering ervan.

2.2. Rapportering, evaluatie en sensibiliseringscampagne

Voor deze beleidslijn moeten de volgende aspecten worden uitgevoerd:

- Elke medewerker wordt regelmatig bewust gemaakt over het belang van toegang tot informatie. Er moet minstens jaarlijks een sensibiliseringscampagne of informatiesessie met betrekking tot informatieveiligheid en privacy opgezet, gevalideerd, gecommuniceerd en opgevolgd worden.
- Er wordt jaarlijks een evaluatie uitgevoerd rond de naleving van dit beleid in de praktijk (via interne enquête).

Bijlage A: Documentbeheer

Versiebeheer

Datum	Auteur	Versie	Beschrijving van de verandering	Datum goedkeuring	Datum in werking treden
2013		V2013	Eerste versie	31/01/2013	01/02/2013
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:

- http://www.iso.org/iso/iso27001
- 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.enisa.europa.eu/topics/data-protection
- https://www.sans.org/security-resources/policies/general/pdf/clean-desk-policy
- http://www.ccb.belgium.be/nl/work
- https://www.safeonweb.be/nl
- https://www.safeinternetbanking.be
- https://www.cybersimpel.be/nl

Bijlage C: Richtlijnen rond clean desk & clear desk

Dankzij de toepassing van "Clean Desk, opgeruimd bureau en leeg scherm" kan het risico worden beperkt op ongeoorloofde toegangen of op beschadiging van de digitale informatiedragers, papieren documenten of andere middelen en van de informatieverwerkingsmiddelen.

De beleidslijnen voor informatieveiligheid en privacy beogen een gepaste veiligheid toe te passen op de werkplaats van de werknemer.

- De netheid binnen de organisatie verhogen:
  - Wanneer alle bureaus en werkruimtes zijn opgeruimd en er nergens papieren rondslingeren, betekent dit een groter comfortgevoel bij de medewerkers en een positieve indruk van de organisatie bij de bezoekers.
- De bescherming van de vertrouwelijke gegevens verbeteren:
  - Een groot deel van de informatie die door de organisatie wordt verwerkt, is vertrouwelijk en moet tegen ongeoorloofde toegangen worden beveiligd.
  - Documenten met gevoelige informatie die men wenst af te drukken, moeten onmiddellijk bij de printers verwijderd worden. Eventueel kan men het afdrukken van documenten beschermen via een persoonlijke code
  - Alle documenten met gevoelige informatie (zoals vertrouwelijke gegevens, klanteninformatie, …) moeten op zodanige wijze opgeborgen worden dat deze enkel toegankelijk zijn voor bevoegde medewerkers
  - Documenten met gevoelige informatie, die niet meer moet bijgehouden worden en die de werknemer wenst te vernietigen, moeten op een veilige manier vernietigd worden. Dragers die gevoelige informatie bevatten, en die niet meer moeten bijgehouden worden, moeten op een zodanige wijze vernietigd worden dat de vertrouwelijkheid van de informatie gevrijwaard wordt.
  - Archiefruimten waarin documenten met vertrouwelijke informatie gearchiveerd worden, moeten altijd op slot zijn
- De productiviteit verhogen:
  - Een opgeruimd bureau zal de productiviteit verhogen omdat er minder tijd verloren gaat bij het zoeken van documenten.
  - Door toepassing van dat beleid kunnen de bureaus door meerdere medewerkers worden gedeeld (“flexdesk”).

In de praktijk

“Clear desk”-richtlijnen promoten de toepassing van drie basisregels:

1. Wanneer de medewerker op kantoor aanwezig is : de medewerker probeert enkel de documenten die hij die dag nodig heeft op zijn bureau te laten liggen.

2. Wanneer de medewerker tijdelijk zijn bureau verlaat: indien de medewerker vaak aan vergaderingen deelneemt, moet hij/zij controleren of er geen vertrouwelijke informatie aanwezig is op zijn bureau die onbewaakt mag worden achtergelaten. Indien dit wel het geval is, moet hij/zij deze informatie veilig opbergen. Bovendien moet hij/zij bij een langere afwezigheid minimaal de computer in slaaptoestand zetten en beveiligen aan de hand van een paswoord.

3. Wanneer de medewerker zijn bureau verlaat: het is de taak van de medewerker om ervoor te zorgen dat alle gevoelige informatie op een veilige plaats wordt opgeborgen zoals een kast die op slot kan en dat zijn bureau is opgeruimd alvorens de organisatie te verlaten. Een tweede sleutel moet bijgevolg worden afgegeven aan een andere dienst of medewerker om indien nodig toegang te hebben tot de documenten. Het behoort tot de verantwoordelijkheid van de medewerkers om de nodige veiligheidsmaatregelen te nemen in hun bureau. Verwerkingsverantwoordelijken moeten nagaan of hun medewerkers dit beleid in acht nemen.

Handige tips ter handhaving van een ordelijke en veilige werkplek:

- Plaats een afspraak in de agenda om op regelmatige tijdstippen de werkplek en papierwerk op te ruimen.
- Bij twijfel over het al of niet bijhouden van een papier of document, is het meestal zo dat het beter is het gewoon op een veilige manier te verwijderen.
- Ga regelmatig door de zaken op een bureau om na te kijken of men ze nog nodig hebt.
- Ruim altijd de werkplek op vooraleer naar huis te gaan.
- Doe archiefkasten op slot op het einde van de werkdag.
- Berg draagbare PC’s altijd op een veilige manier op.
- Gebruik papierversnipperaars voor gevoelige documenten die niet meer nodig zijn en wenst te vernietigen.
- Media waarop gevoelige informatie opgeslagen wordt zoals CDs, DVDs, externe harde schijven of USB-sleutels, moeten ook op een veilige manier opgeborgen worden en moeten verwijderd worden van de werkstations.
- Overweeg om papieren of documenten in te scannen en elektronisch te bewaren en de papieren of documenten naderhand op een veilige manier te vernietigen.
- Na het beëindigen van een vergadering de borden wissen en de ingevulde flip-charts verwijderen.
- Het neerschrijven van user IDs en volledige wachtzinnen en achterlaten op het bureau is niet toegelaten.

Toegang tot de informatie

Media moeten zorgvuldig door de gebruiker worden beheerd: prints, brieven, USB-sleutels, back-upschijven, gedeelde bestanden, pc, tablet, ... De gebruiker kan bijvoorbeeld gegevens afdrukken die afkomstig zijn van een toepassing die door middel van de elektronische identiteitskaart is beveiligd. In dat geval is de afgedrukte versie van deze gegevens anders te beveiligen. Hieronder volgen nog enkele tips.

- De documenten met gevoelige gegevens worden bij voorkeur afgedrukt na het intypen van een code waardoor ze niet direct uit een printer komen en onbewaakt achterblijven. Medewerkers kunnen dan aan de printer alsnog beslissen om documenten niet af te drukken (ook goed voor lager tonerverbruik en voor het milieu).
- Elke USB-sleutel kan worden gebruikt om documenten van het ene systeem naar het andere over te zetten. Wanneer gevoelige gegevens worden overgemaakt, moet de USB-sleutel idealiter volledig vercijferd worden en moeten de gegevens die hierop werden opgeslagen onmiddellijk na de overzetting verwijderd worden. Alternatief is de gevoelige informatie in een ZIP file stoppen met een paswoord.
- Elke back-up op gelijk welk medium (SD drive, CD, DVD, USB-sleutel, externe harde schijf,...) moet in een fysiek beveiligde omgeving worden bewaard en mag nooit onbewaakt worden achtergelaten.
- Een vernietigingssysteem voor vertrouwelijke of gevoelige documenten is beschikbaar voor elke medewerker.
- Geen enkel persoonsgegeven mag via e-mail worden overgemaakt in zichtbare vorm. Alvorens gevoelige bestanden per e-mail worden verstuurd, moet ervoor worden gezorgd dat deze bestanden goed vercijferd zijn.
- In het geval van gedeelde mappen met gevoelige gegevens voor een bepaald publiek, moeten deze mappen op het niveau van de toegangsrechten duidelijk geconfigureerd worden.
- Gevoelige gegevens op een printer of bureau achterlaten is niet toegelaten.

Bijlage E: 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	
Aankopen, onderhouden en ontwikkelen van informatiesystemen	
Leveranciersrelaties	
Beheer van veiligheidsincidenten	
Informatieveiligheidsaspecten van continuïteitsbeheer	
Naleving	

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