Beleidslijn informatieveiligheid en privacy

Email, online communicatie en internet gebruik

(BLD ONLINE)

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 bevat beleidslijnen met betrekking tot het gebruik van e-mail, online communicatiemiddelen en internet toegang die ter beschikking gesteld worden van de medewerker. De medewerker speelt een wezenlijke rol in de veiligheid van de organisatie in het algemeen. De medewerker staat in de eerste verdedigingslinie voor wat de risico's bij de verwerking van professionele en gevoelige informatie betreft. Daarom is het belangrijk dat elke medewerker zich terdege bewust is van zijn rechten en plichten op dat vlak en van de goede praktijken binnen de organisatie.

2. Email, online communicatie en internet gebruik

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

a. Elke organisatie moet de regels verwerken in hun beleid voor informatieveiligheid en privacy die gespecifieerd zijn in bijlage C van de beleidslijn ‘Email, online communicatie en internet gebruik’. Deze regels zijn beschreven in de paragrafen :
   1. gebruiken van e-mail en online communicatiemiddelen
   2. veilig gebruik van internet

b. Elke organisatie moet een permanente controle uitoefenen op email, online communicatie en internet gebruik in het kader van de volgende doelstellingen:
   1. de bescherming van de reputatie en de belangen van de organisatie;
   2. het voorkomen van ongeoorloofde handelingen of handelingen die indruisen tegen de goede zeden of die de waardigheid van een persoon kunnen schaden;
   3. de veiligheid en/of de goede technische werking van de netwerksystemen van de organisatie, met inbegrip van de beheersing van de eraan verbonden kosten, alsook de fysieke beveiliging van de installaties van de organisatie;
   4. de naleving van de kernprincipes.

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.safeonweb.be/nl
- https://www.safeinternetbanking.be

Bijlage C : Email, online communicatie en internet gebruik

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

Algemene beleidslijn

Zoals voor alle werkinstrumenten geldt, is het gebruik van de communicatiemiddelen en werkmiddelen van de organisatie in principe voorbehouden voor beroepsdoeleinden. Echter, het gebruik van e-mail, online communicatiemiddelen en internet voor privédoeleinden wordt in beperkte mate toegestaan, op voorwaarde dat het gaat om een occasioneel gebruik en dat dit de goede werking van het netwerk, het werk en de productiviteit niet in het gedrang brengt en het geen inbreuk inhoudt op de wetgeving.

Voor beroepsmatige communicaties aanvaardt de organisatie enkel het gebruik van de e-mail, online communicatie diensten en internet diensten die eigen zijn aan de organisatie. Andere online communicatiemiddelen (zoals blogs, vlogs, chat, WhatsApp, Telegram, WeChat, BBM) en andere internet diensten (zoals Facebook, Linkedin, Twitter, Instagram, Wikipedia, Youtube) mogen enkel worden gebruikt voor zover de interne richtlijnen omtrent het gebruik van deze communicatiemiddelen het toelaat. De medewerker zal de regels voor het gebruik van deze middelen en diensten strikt in acht nemen.

De medewerker verbindt zich ertoe de slechte werking of het misbruik van de e-mail, online communicatie en internet functionaliteiten (zoals virussen, malware, pogingen tot hacking en phishing), ongeacht of dit op het niveau van de centrale computers, het netwerk, de website, de lokale computers of de software is, onmiddellijk mee te delen.

De directie van de organisatie behoudt zich het recht voor om het gebruik van e-mail, online communicatiemiddelen en internet te controleren.

Gebruiken van e-mail en online communicatiemiddelen

Gelet op de inherente risico's[1] die verbonden zijn aan het gebruik van e-mail binnen de organisatie, is het belangrijk om de beleidslijnen in herinnering te brengen:

- De verzender van een e-mail is verantwoordelijk voor de inhoud van dit bericht. Het is de medewerkers strikt verboden om e-mails te verzenden waarvan de inhoud onwettig zou zijn en/of in strijd met het fatsoen en de zeden (zoals e-mails met een aanstootgevende, politieke, racistische, discriminerende inhoud).
- E-mail en andere online communicatiemiddelen mogen niet gebruikt worden ter vervanging van de uitwisselingsmethoden die door de Kruispuntbank van de Sociale Zekerheid (KSZ) opgelegd worden voor de uitwisseling van persoonsgegevens. Het gebruik van e-mail en online communicatiemiddelen dient te gebeuren in overeenstemming met de aanbevelingen inzake de bescherming van de persoonlijke levenssfeer. Dus mogen er geen persoonsgegeven zonder afdoende veiligheidsmechanismen via e-mail en online communicatie middelen worden overgemaakt. Alvorens gevoelige bestanden via e-mail en online communicatiemiddelen te versturen, dient de medewerker ervoor te zorgen dat deze bestanden goed vercijferd zijn.
- Het gebruik van e-mail en online communicatie middelen voor persoonlijke doeleinden is toegelaten met mate. Dit gebruik voor privé-aangelegenheden mag echter geen inbreuk op deze beleidslijn inhouden, noch op enige andere wettelijke of reglementaire bepaling. Als de medewerker zijn e-mail en online communicatie middelen voor persoonlijke doeleinden gebruikt, dient hij in de mate van het mogelijke elke verwijzing naar zijn werkgever te verwijderen om aldus verwarring te vermijden met het beroepsmatige gebruik van de e-mail (de vermelding "Prive" of “Persoonlijk” toevoegen in het onderwerp van het bericht).
- Bij langdurige afwezigheid van de medewerker (meerdere dagen) dient een automatisch antwoord ingesteld te worden zodat correspondenten op de hoogte zijn van de langedurige afwezigheid ("out of office"). Idealiter geldt deze maatregel enkel voor bestemmelingen binnen de sociale zekerheid.

[1] de waarschijnlijkheid dat een negatieve impact zich zal voordoen wanneer er geen beschermingsmaatregelen genomen worden

- De medewerker zal geen e-mails naar grote groepen medewerkers versturen ("To All Users") en zal geen grote bestanden toevoegen die de werking van het systeem kunnen hinderen, tenzij de medewerker hiervoor gemandateerd is (lid van de interne communicatiedienst). Grote bestanden worden bij voorkeur op het interne documentbeheersysteem van de organisatie geplaatst. De e-mail bevat enkel een link naar de bestanden.
- Het is verboden om ontvangen e-mails systematisch door te sturen naar externe bestemmelingen (e-mail adres of online communicatiemiddel buiten de organisatie), omdat ook professionele en gevoelige informatie automatisch verstuurd worden naar deze externe bestemmelingen.

Veilig gebruik van internet

Internet wordt in de eerste plaats ter beschikking gesteld voor professionele doeleinden. Het verkennen van internet voor persoonlijke vorming en ontwikkeling wordt aanvaard mits het in beperkte mate gebeurt. In dat opzicht dient de medewerker zich ervan bewust te zijn van de volgende beleidslijnen :

- de organisatie behoudt zich het recht voor om de toegang tot internet (websites en diensten) te beperken;
- surfen op internet houdt risico's in en de kans op een aanval via bepaalde sites is realistisch. De medewerker moet:
  - steeds bewust zijn dat hij/zij de organisatie vertegenwoordigt op internet. Veel websites houden een spoor bij van bezoek en kunnen soms de herkomst en de elektronische identiteit vaststellen van de persoon en van de organisatie;
  - de configuratie van de webbrowser en de beveiligingssoftware (antivirus, antispam, firewall) zoals ingesteld door de organisatie ongewijzigd houden.
  - niet-professionele sites verlaten bij vermoeden dat de bezochte site niet is waar naar gezocht werd.
- het is verboden websites te raadplegen waarvan de inhoud indruist tegen de goede zeden of de waardigheid van een persoon kan schaden, alsook racistische websites, websites die discriminatie voorstaan op basis van geslacht, seksuele geaardheid, handicap, religie of politieke overtuiging.
- het is verboden om internet te gebruiken voor illegale activiteiten, ongeacht de aard ervan.
- bij het downloaden van bestanden beperkt de medewerker zich tot het strikt noodzakelijke in het kader van zijn beroepsactiviteiten, voor zover de organisatie het downloaden toestaat.
- een medewerker maakt geen gebruik van onveilige online file-sharing diensten die toelaten om veel en/of grote bestanden te delen en op te laden (zoals Dropbox, Onedrive, iCloud, GoogleDrive, Box, WeTransfer, ShareFile, Nomadesk). De medewerker moet voorafgaandelijk nagaan bij de veiligheidsconsulent welke online file-sharing diensten wel veilig en toegelaten zijn of welke tools de medewerker moet gebruiken om bestanden veilig uit te wisselen.
- een medewerker moet op voorhand nagaan of een softwareprogramma afkomstig is van een betrouwbare bron, of er geen tegenstrijdigheid bestaat met het licentiebeleid van de organisatie en of er een risico bestaat op het vlak van informatieveiligheid of privacy, alvorens dergelijk softwareprogramma te installeren.

Controle

De organisatie moet een permanente controle uitoefenen in het kader van de volgende doelstellingen:

1. de bescherming van de reputatie en de belangen van de organisatie;
2. het voorkomen van ongeoorloofde handelingen of handelingen die indruisen tegen de goede zeden of die de waardigheid van een persoon kunnen schaden;
3. de veiligheid en/of de goede technische werking van de netwerksystemen van de organisatie, met inbegrip van de beheersing van de eraan verbonden kosten, alsook de fysieke beveiliging van de installaties van de organisatie;
4. de naleving van de kernprincipes.

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	**Ja**
Cryptografie	
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 *****