slachtoffer HULP NEDERLAND

ICT-gebruiksreglement

Inhoud

Inleiding

We leven in een tijd waarin de ontwikkelingen in de informatietechnologie razendsnel gaan. Dit biedt nieuwe mogelijkheden om onze dienstverlening te verbeteren. Tegelijkertijd geeft het de kwaadwillende steeds meer opties om informatietechnologie voor verkeerde doelen te gebruiken.

Iedereen die gebruikmaakt van ICT-middelen laat een digitaal spoor achter. Vandaar dat het belangrijk is dat jij integer en effectief met onze ICT-middelen omgaat. Het gebruik van privé-middelen voor werk gerelateerde e-mails, telefoongesprekken of documentenopslag is niet toegestaan omdat Slachtofferhulp Nederland niet kan garanderen dat deze middelen voldoende beveiligd zijn. Laten we er samen voor zorgen dat de privacy van cliënten, relaties en medewerkers goed wordt beschermd. Dit helpt ook om (secundaire) victimisatie te voorkomen.

Vanaf het moment dat jij gebruikt maakt van onze ICT-middelen, word je geacht je te houden aan dit ICT-gebruiksreglement. Lees het daarom zorgvuldig door. Op deze manier beperken we de risico's die het gebruik met zich meebrengt tot een minimum. Door het ondertekenen van je contract accepteer je ook deze voorwaarden

Het ICT-gebruiksreglement

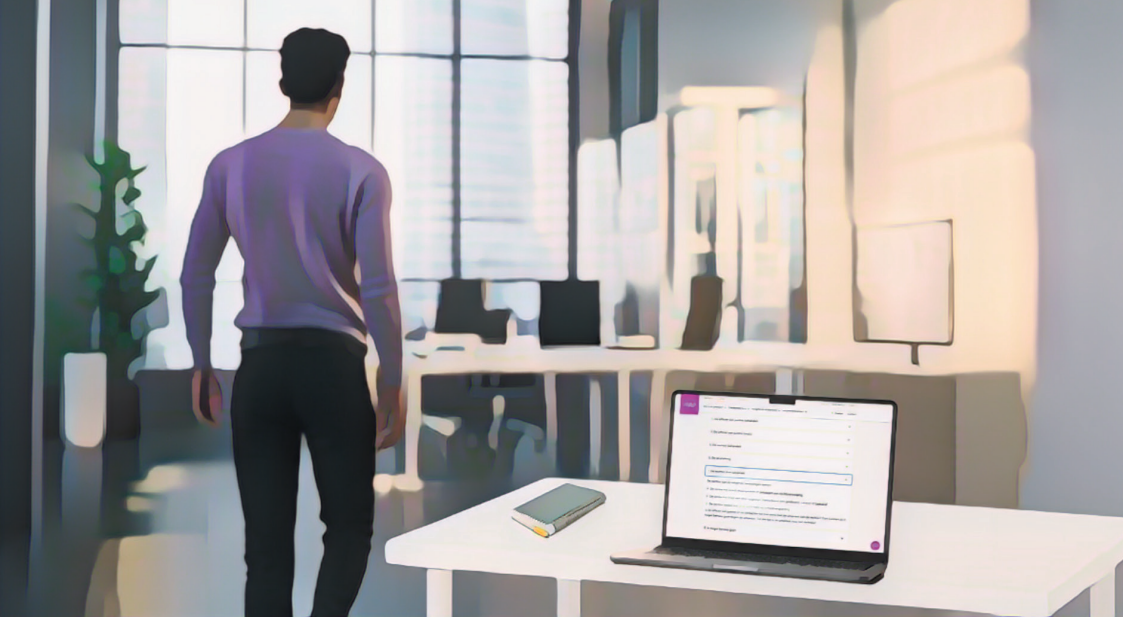
1. Eigendom ICT-middelen

Alle ICT-middelen die aan jou worden verstrekt, blijven eigendom van Slachtofferhulp Nederland. Je ontvangt de ICT-middelen in bruikleen voor de duur van je arbeidsovereenkomst of gedurende de periode waarin jij voor ons werkzaam bent. De in bruikleen gegeven middelen worden geregistreerd in Topdesk door het Servicepunt. Onderling ruilen van apparatuur is niet toegestaan.

Uiteraard ga je zorgvuldig om met onze ICT-middelen en houd je je aan de bijbehorende gebruiksaanwijzingen. Mocht er toch schade ontstaan door opzet of grove nalatigheid bij het gebruik, dan kunnen wij de schade op jou verhalen.

Alle geregistreerde ICT-middelen worden gemonitord op afwijkingen. Dit kan invloed hebben op je privacy. De maatregelen zijn echter essentieel om te voldoen aan de veiligheidseisen voor persoonsgegevens en de richtlijnen van de Autoriteit Persoonsgegevens (AP).

Als je contract eindigt, lever je de verstrekte ICT-middelen in bij het Servicepunt op het Landelijk kantoor. Het Servicepunt zorgt voor de correcte verwerking in het registratiesysteem, zodat de in bruikleen gegeven middelen niet meer op jouw naam staan. Tot dat moment ben je verantwoordelijk voor de ICT-middelen. Slachtoffferhulp Nederland kan kosten in rekening brengen als je de in bruikleen gegeven apparatuur niet inlevert.



2. Gebruik van (draagbare) apparatuur

Om de veiligheid van gegevens te waarborgen, zijn de volgende regels voor het gebruik van apparatuur van belang:

- Je bent zelf verantwoordelijk voor de staat waarin de ICT-middelen verkeren die je in bruikleen hebt. Denk hierbij aan verstandig omgaan met het gebruik van het middel, en - bij storingen - tijdig onderhoud aanvragen, zodat eventuele schade tot een minimum wordt beperkt.
- Het is niet toegestaan om zelf veranderingen aan te brengen aan de standaard beveiligings- en netwerkverbindingsinstellingen van een mobiele telefoon, laptop of werkstation van Slachtofferhulp Nederland.
- Onze mobiele devices, zoals mobiele telefoons, zijn voorzien van een Mobile Device Management-beheeroplossing. Dit betekent dat Slachtofferhulp Nederland het toestel beheert en bepaalt welke apps hierop kunnen worden geïnstalleerd. Als installatie van een specifieke app noodzakelijk is, gebeurt dit in overleg met de afdeling Informatievoorziening.
- Plaats draagbare ICT-middelen als je ze niet gebruikt (binnen én buiten Slachtofferhulp Nederland) in een afgesloten ruimte of kamer. Laat draagbare ICT-middelen dus niet onbeheerd achter in een openbare (vrij toegankelijke) ruimte of in een voertuig.
- Bij het verlaten van je werkplek ben je verplicht om je werkstation te vergrendelen, bijvoorbeeld via de toets-combinatie  of Ctrl-Alt-End+ Enter.

- Beveilig mobiele devices, zoals mobiele telefoons, altijd met een code van minimaal vijf karakters. Je mag deze code niet verwijderen. Gebruik van veegpatronen en eenvoudig te raden pincodes zoals 00000 of 12345 zijn niet toegestaan.
- Bewaar wachtwoorden niet in de buurt van ICT-middelen.

3. Gebruik van programmatuur

De softwarepakketten die wij gebruiken en beheren, worden centraal beschikbaar gesteld aan de medewerkers. Wij hanteren de volgende regels voor het gebruik van deze programmatuur:

- Programmatuur installeren op onze middelen is alleen toegestaan met toestemming van de afdeling Informatievoorziening. Zo voorkomen we dat de systemen met virussen of malware worden besmet of dat de integriteit van de werkplek wordt geschonden.
- Gebruik het toegewezen werkstation en alle andere verstrekte ICT-middelen alleen voor je werkzaamheden bij onze organisatie. Gebruik van spelletjes, films kijken, privé-programmatuur en dergelijke zijn niet toegestaan.
- Je mag geen illegale programmatuur of content beheren, downloaden en/of installeren op de harde schijf van het toegewezen werkstation, de persoonlijke U-schijf en op usb-sticks en andere media van Slachtofferhulp Nederland.
- Je mag niet zelf programmatuur kopiëren of licenties installeren (ook niet naar je eigen directory op het netwerk, of naar een harddisk of usb-stick).

4. Web-toepassingen, AI-toepassingen en applicaties
(niet beheerd door Slachtofferhulp Nederland)

Een speciale vorm van programmatuur zijn generieke beschikbare applicaties en gebundelde applicaties.

- Generiek beschikbare applicaties zijn: applicaties die niet geïnstalleerd hoeven te worden, maar die je via een externe website kan benaderen en gebruiken. Denk daarbij aan WeTransfer, ChatGPT en Deepl.
- Gebundelde applicaties zijn applicaties die als onderdeel van een andere, maar benodigde, applicatie meekomen en niet echt geblokkeerd kunnen worden. Denk aan WhatsApp, Signal, OneDrive en SharePoint.

Deze programmatuur of applicaties, al dan niet geïnstalleerd op ICT-middelen, worden niet door ons beheerd en ondersteund en mogen niet worden gebruikt voor het opslaan, verzenden, vertalen, etc. van persoonsgegevens.

5. Omgang met persoonsgegevens

Door het tekenen van je (arbeids)overeenkomst, teken je tegelijkertijd een geheimhoudingsverklaring.

- Houd je aan de werkinstructie "veilig omgaan met informatie d.m.v. classificatie" bij het verwerken (zoals lezen, opslaan, verspreiden, ect.) van zakelijke en/of privacygevoelige (persoons)gegevens die betrekking hebben op individuele slachtoffers, medewerkers en onze bedrijfsvoering.
- Bewaar persoonsgegevens alleen in geprinte vorm als dit in overeenstemming is met het beleid 'Veilig Thuis Werken met persoonsgegevens van slachtoffers, thuis en onderweg'.
- Je mag niet ongeautoriseerd en zonder overleg op ons netwerk databestanden of gegevens van cliënten verwijderen, onherkenbaar en/of onbruikbaar maken.
- Verstuur geen privacygevoelige informatie onversleuteld via e-mail naar (publieke) adressen buiten ons domein. Informatie mag in principe alleen versleuteld per e-mail verstuurd worden aan personen die geautoriseerd zijn voor de betreffende informatie. Maak daarbij gebruik van Cryptshare.
- Mochten er procesproblemen zijn, denk aan het uitwisselen van sleutels, met JuBIT ketenpartners zoals OM en Politie dan mag de e-mail (alleen gericht aan [email]@om.nl en [email]@politie.nl) onversleuteld worden verstuurd.

- Raadpleeg persoonsgegevens van slachtoffers uitsluitend als dit noodzakelijk is voor de hulpverlening en dienstverlening aan het slachtoffer, of voor een van de andere doeleinden waarvoor wij persoonsgegevens verwerken.
- Schrijf geen gegevens weg op privé-apparatuur. Dit is in strijd met de geheimhoudingsplicht. Wij zijn anders niet in staat om passende (organisatorische) maatregelen te treffen, zoals een gecontroleerde back-up.
- Gebruik van web-toepassingen, AI-toepassingen en applicaties die niet door ons beheerd worden, zoals Whatsapp en SMS, wordt sterk afgeraden vanwege de veiligheid van gegevens. Er mogen geen (bestanden met) privacygevoelige (persoons)gegevens worden verwerkt of verzonden via deze web-toepassingen.

6. Gebruikersnamen, wachtwoorden en rechten

Om informatiesystemen en gegevens te kunnen gebruiken, krijg je een uniek user-ID en een bijbehorend wachtwoord. Bij gebruik van meerdere systemen kunnen daar andere wachtwoorden bijkomen.

- Je wachtwoord is strikt persoonlijk. Je mag dit niet doorgeven aan andere personen, ook niet aan collega's.
- Wijzig je wachtwoorden minimaal elke 45 dagen om misbruik te voorkomen.
- Vul je vijf keer een fout wachtwoord in, dan blokkeert het beveiligingssysteem automatisch je algemene gebruikersaccount. Open Line Servicedesk kan je gebruikersaccount weer vrijgeven.
- Let bij het omgaan met wachtwoorden op het volgende:
  → Schrijf wachtwoorden niet op. Bewaar ze niet in de buurt van ICT-middelen.
  → Gebruik zogenaamde 'sterke wachtwoorden', dit houdt in:
    - Niet gemakkelijk te raden, bijvoorbeeld geen naam van je partner, kind of huisdier.
    - Wel gemakkelijk te onthouden, bijvoorbeeld de eerste letters of titel van een boek + cijfers.
    - Minimaal 10 karakters.

  Tip: gebruik een zin.
- Ga bewust om met toegangsgegevens zodat je daarmee geen onbevoegden stimuleert om toegang te krijgen tot ons netwerk.

Om systemen en gegevens te kunnen benaderen, zijn rechten nodig. Deze rechten zijn gebaseerd op functie-inhoud, beschreven in de functiebeschrijving, en gaan in bij indiensttreding. Aanvullende rechten kan je leidinggevende voor je aanvragen, met toestemming van de systeemeigenaar (Slachtofferhulp Nederland). Voor vragen hierover je terecht bij de functioneel beheerder of, als deze niet bekend is, Open Line Servicedesk (088-500 6736).

7. Antivirus & Malware

De volgende (gedrags-)regels zijn belangrijk om virussen te voorkomen:

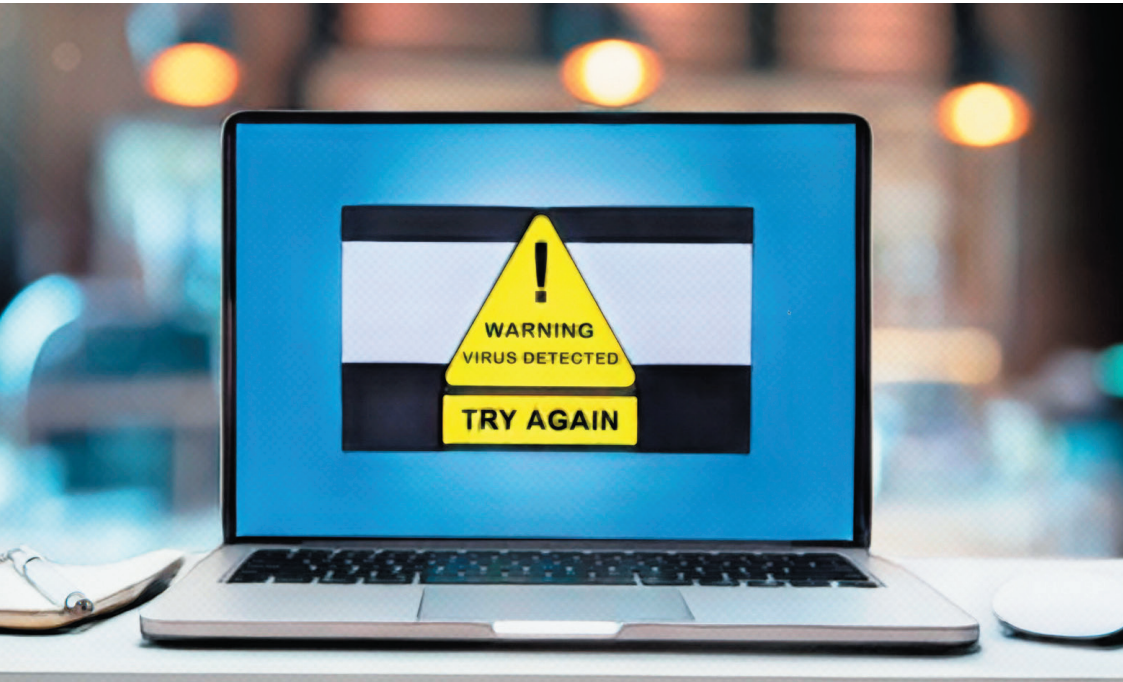
- Gebruik uitsluitend programmatuur die wij hebben geïnstalleerd.
- Zet je virusscanner nooit uit.
- Klik nooit op een link als er geen noodzaak toe is. Is er wel noodzaak: verifieer de authenticiteit en bedoelingen van de verzender. Bijvoorbeeld door de verzender hierover te bellen.
- Open nooit verdachte e-mails. Maak een print screen en stuur deze naar Open Line Service Portaal. Verwijder de verdachte e-mail direct na het maken van een print screen.

Tips: zo herken je een virus en/of malware

- Gegevens in of bestandsnamen van documenten zijn op onverklaarbare wijze verminkt.
- Het werkstation is zonder reden erg traag.
- Onverwachte activiteit op harde schijf, U-schijf of M-schijf.
- Storingen op het beeldscherm, vreemde teksten of tekens.
- De beschikbare geheugenruimte wordt plotseling minder of de harde schijf loopt vol.

Wat te doen bij een (mogelijke) virusinfectie?

- Stop elke handeling met het werkstation.
- Noteer je laatste werkzaamheden met het werkstation.
- Schakel je werkstation uit als deze aan het netwerk is gekoppeld.
- Laat niemand meer toe tot je werkstation.
- Neem direct contact op met Open Line Servicedesk.
- Neem ook contact op met het Data Protectie Team (Privacy@slachtofferhulp.nl).
- Probeer nooit het virus of de malware zelf onschadelijk te maken of te verwijderen.



Als je via het thuiswerkportaal en een laptop (eigen computer of van Slachtofferhulp Nederland) werkt, moet je regelmatig de updates van de virusdefinities installeren via de automatische updatefunctie. Vernieuw, wanneer nodig, de antivirussoftware. Bij vragen bel of mail je Open Line Servicedesk (088-500 6736).

8. E-mail, documentenopslag (U- /M-schijf, one-drive en Teams / SharePoint) en internetprotocol

Binnen onze organisatie geldt een aantal regels voor het gebruik van e-mail, de U-/M-schijf, OneDrive, Teams en internet:

- Gebruik e-mail, de U-/M-schijf, OneDrive, Teams en internet niet voor doeleinden die in strijd zijn met de wet of met onze kernwaarden, of die tegengesteld zijn aan onze belangen.
- Beperkt persoonlijk gebruik van e-mail, de U-/M-schijf, OneDrive, Teams en internet is wel toegestaan, mits dit niet storend is voor je dagelijkse werkzaamheden.
- Verzend, ontvang en archiveer geen informatie op eigen initiatief die discriminerend, kwetsend, beledigend, bedreigend, obsceen of pornografisch is, of die denigrerend is over huidskleur, geslacht, leeftijd, handicap, godsdienst, nationaliteit, uiterlijk of seksuele voorkeur van een persoon of groep.
- Verzend via ons e-mailsysteem geen ‘algemene berichten’ met commerciële strekking die niet ten behoeve van het zakelijk verkeer zijn.
- Verzend niet anoniem of onder een fictieve naam berichten. Je mag ook niet zonder toestemming gebruikmaken van middelen om informatie te beveiligen zonder dat wij in staat zijn kennis te nemen van de inhoud van het bericht.
- Je mag niet online gokken of kettingbrieven versturen.
- Materialen met auteursrecht kopiëren, wijzigen, verzenden of opslaan is alleen toegestaan met toestemming van de eigenaar van het auteursrecht.
- Vertrouwelijke of gevoelige bedrijfsspecifieke informatie verstrekken mag alleen in overleg met je leidinggevende.
- Voor het registreren, verzamelen, controleren, combineren of bewerken van informatie moet je ons privacyreglement en ons privacybeleid in acht nemen.

- Open niet zonder toestemming e-mailberichten van andere gebruikers.
- Bij geplande afwezigheid ben je zelf verantwoordelijk voor het instellen van je afwezigheidsmelder. Je zorgt in overleg met je leidinggevende voor een overdracht. Vanwege het privékarakter van je e-mailberichten, de U-schijf, OneDrive en je telefoon en het recht op privacy kunnen wij in slechts uitzonderlijke gevallen en onder strenge voorwaarden toegang verschaffen tot je mailbox, U-schijf, OneDrive en telefoon. Uitgebreide informatie vind je in de privacyverklaring.

Heimelijke controle

Wij hebben de bevoegdheid om het gebruik van je telefoon, e-mail, de U-/M-schijf, OneDrive, Teams(SharePoint) en van het internet zo nodig te monitoren en te controleren. Generieke controles zullen in beginsel alleen plaatsvinden op het niveau van getotaliseerde gegevens die niet herleidbaar zijn tot identificeerbare personen. Als er sprake is van een redelijke verdenking dat je iets doet wat strafbaar of verboden is, heeft het hoofd HRM de bevoegdheid om, in overleg met de Privacy Officer, hiernaar specifiek onderzoek te verrichten. Het hoofd HRM informeert de Raad van Bestuur over dit besluit. De betrokken medewerker kan indien nodig een klacht indienen over het onderzoek op grond van het 'Klachtenreglement Privacy', te vinden op de 'Werkwijzer' van ons intranet 'de Binnenplaats'.

Bij controle conformeren wij ons aan de voorwaarden die voortvloeien uit de privacywetgeving (zie privacy verklaring).

9. Printen/opslaan van documenten

Wij zijn verplicht de persoonsgegevens van onze cliënten en medewerkers te waarborgen.

- Je mag niet zonder onze toestemming thuis afdrukken maken van gegevens uit het CRM, de Binnenplaats of van andere gegevens die privacygevoelige informatie bevatten.
- Ook mag je geen bestanden met privacygevoelige informatie en/of gegevens uit het CRM of de Binnenplaats op je lokale computer bewaren of naar een extern (privé) e-mailadres versturen.

Indien noodzakelijk wissel je vertrouwelijke informatie alleen uit via je zakelijke e-mailadres. Hierbij benadrukken we dat je:

- Alle zaak-gerelateerde gegevens (inclusief scans van fysieke documenten) zo snel mogelijk in het clientregistratiesysteem zet (of de hele e-mail daarin kopieert), waarna je de e-mail uit je mailbox verwijdert.
- Alle fysieke documenten en e-mails van een zaak zo snel mogelijk (en anders binnen vijf dagen na afsluiting van de zaak) vernietigt (in de shredder/blauwe afgesloten container).
- Voor bestandsuitwisseling gebruik maakt van de daarvoor beschikbaar gestelde tool Cryptshare. Informatie over het gebruik van Cryptshare is te vinden op de Binnenplaats.

Gebruik van draagbare media (zoals een dvd, cd-rom, usb-stick of externe harde schijf) is alleen toegestaan op de door ons goedgekeurde draagbare media, zoals encrypted usb-sticks of een encrypted harddisk. Als je (bijvoorbeeld bij thuiswerken) privacygevoelige gegevens via privé-ICT-middelen in de openbaarheid brengt, ben je zelf verantwoordelijkheid en aansprakelijk voor verlies, diefstal of onrechtmatige raadpleging door derden.

10. Melden van beveiligingsincidenten en verlies of diefstal

Indien je hiermee te maken krijgt, ben je zelf verantwoordelijk voor het zo tijdig mogelijk melden van het incident. Dit doe je als volgt:

- Technische ondersteuning en kwetsbaarheden in de beveiliging:
  → Meld deze via het serviceportaal van Open Line of bel naar 088-500 6738.

- Verlies of diefstal van de in bruikleen gegeven apparatuur:
  → Doe aangifte bij de politie en stuur de aangifte door naar het servicepunt van Slachtofferhulp Nederland.
  → Bel met Open Line om de apparatuur te laten blokkeren, tel. 088-500 6736.
  → Meld het bij je leidinggevende, zodat deze bij het servicepunt vervangende apparatuur kan regelen. Tel. 088-7460124.

- Privacy gerelateerde zaken:
  → Neem contact op met de Privacy Officer via het e-mailadres: privacy@slachtofferhulp.nl.

Sla bovenstaande gegeven op je privé toestel of elders op, zodat je de gegevens bij de hand hebt als zich een incident voordoet.

Gebruikte definities

ICT-middelen	Apparatuur, programmatuur, licenties die Slachtofferhulp Nederland beschikbaar stelt om de werkzaamheden te kunnen uitoefenen.
CRM	Cliënt Relatie Systeem,
Apparatuur	Werkstations, printers, beamer, mobiele en vaste telefoons.
Werkstations	Thin Clients, mobiele Thin Clients, Chromebooks, desktops en laptops.
Mobiele devices	Mobiele telefoons en tablets.
Medewerker/werknemer	Iedereen die op basis van een overeenkomst met Slachtofferhulp Nederland werkzaamheden verricht voor Slachtofferhulp Nederland.

Slachtofferhulp Nederland

Vandaag verder