slachtoffer HULP NEDERLAND

ICT Gebruiksreglement & Bruikleenovereenkomst

Slachtofferhulp Nederland en Perspectief Herstelbemiddeling

Inleiding

Iedereen die bij Slachtofferhulp Nederland werkt en gebruikmaakt van de beschikbaar gestelde ICT-middelen, moet zich houden aan dit ICT-gebruiksreglement.
Dit geldt voor betaalde en onbetaalde medewerkers, en ook voor derden (zoals freelancers) die van Slachtofferhulp Nederland ICT-middelen beschikbaar krijgen gesteld.
Dit ICT-gebruiksreglement is bedoeld om zo efficiënt en effectief mogelijk om te gaan met de ICT-middelen en tegelijkertijd de risico's bij het gebruik zoveel mogelijk te verkleinen.

Elke medewerker/derde ontvangt dit ICT-gebruiksreglement samen met het contractvoorstel voor indiensttreding of aanvang van werkzaamheden.
De medewerker/derde wordt erop gewezen dat hij/zij met het tekenen van het contract ook het ICT-reglement accepteert.

Het ICT-gebruiksreglement

Eigendom ICT-middelen

Alle ICT-middelen die Slachtofferhulp Nederland verstrekt zijn eigendom van Slachtofferhulp Nederland. De medewerker krijgt deze ICT-middelen in bruikleen gedurende zijn/haar arbeidsovereenkomst, gedurende de periode waarin hij/zij voor Slachtofferhulp Nederland werkt of gedurende de overeengekomen periode. Dit wordt vastgelegd door het Servicepunt. Onderling ruilen van apparatuur is niet toegestaan.

Bij vertrek moet je de verstrekte ICT-middelen en ICT-producten inleveren bij het Servicepunt op het Landelijk kantoor of bij de leidinggevende. Het Servicepunt maakt dan de eerdere vastlegging van de bruikleen ongedaan. Tot die tijd ben je als medewerker eindverantwoordelijk. Slachtofferhulp Nederland kan kosten in rekening brengen als je niet in staat bent de in bruikleen gegeven apparatuur of software in te leveren.

Gebruik van (draagbare) apparatuur

- Je mag draagbare ICT-middelen in een openbare (vrij toegankelijke) ruimte niet onbeheerd achterlaten.
- Je mag draagbare ICT-middelen niet onbeheerd in een voertuig achterlaten.
- Je moet zelf draagbare ICT-middelen binnen én buiten Slachtofferhulp Nederland in een afgesloten ruimte of kamer plaatsen als je ze niet gebruikt.
- Bij het verlaten van je werkplek ben je verplicht om je werkstation te vergrendelen, bijvoorbeeld via de toets-combinatie ⊞ + L of Ctrl-Alt-End+ Enter.
- Je bent verantwoordelijk voor de staat waarin de ICT-middelen die je in bruikleen hebt verkeren. Hieronder verstaan we 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.
- Mobiele devices van Slachtofferhulp Nederland (zoals mobiele telefoons) moet je altijd beveiligen 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.

- Mobiele devices van Slachtofferhulp Nederland (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 Informatievoorziening.
- Je mag een e-mailaccount van Slachtofferhulp Nederland op een privé-mobiele telefoon alleen gebruiken in combinatie met Mobile Device Management. Het toestel valt dan onder beheer van Slachtofferhulp Nederland.
- Je mag wachtwoorden niet bewaren in de buurt van ICT-middelen.

Gebruik van programmatuur

Slachtofferhulp Nederland hanteert de volgende regels voor het gebruik van programmatuur:

- De meeste softwarepakketten die Slachtofferhulp Nederland in gebruik heeft, stellen we centraal aan de medewerkers beschikbaar.
- Het is niet toegestaan op een andere manier dan hierboven (eigenhandig) software op laptops of werkstations van Slachtofferhulp Nederland te installeren.
- Je mag het toegewezen werkstation en andere verstrekte ICT-middelen alleen gebruiken voor werkzaamheden voor Slachtofferhulp Nederland. 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).

Omgang met (privacygevoelige) persoonsgegevens

- Met de arbeidsovereenkomst, stageovereenkomst, overeenkomst onbetaalde medewerker of overeenkomst van opdracht teken je tegelijkertijd een geheimhoudingsverklaring.
- Zakelijke en/of privacygevoelige gegevens die betrekking hebben op individuele slachtoffers, medewerkers en de bedrijfsvoering van Slachtofferhulp Nederland, mag je op geen enkele manier opslaan, e-mailen of via post of op andere manieren verspreiden, behalve via de apparatuur, applicatie(s), zakelijke distributiekanalen en/of netwerklocaties die Slachtofferhulp Nederland daarvoor beschikbaar stelt.
- Je mag niet ongeautoriseerd en zonder overleg op het netwerk van Slachtofferhulp Nederland databestanden of gegevens van cliënten verwijderen, onherkenbaar en/of onbruikbaar maken.
- Je mag geen privacygevoelige informatie onversleuteld via e-mail versturen naar (publieke) adressen buiten het domein van Slachtofferhulp Nederland. Informatie mag in principe alleen versleuteld per e-mail verstuurd worden aan personen die geautoriseerd zijn voor de betreffende informatie. Daarbij moet je gebruikmaken van de middelen die Slachtofferhulp Nederland daarvoor ter beschikking stelt (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.
- Persoonsgegevens mag je alleen in geprinte vorm bewaren als dit in overeenstemming is met het beleid ‘Veilig Thuis Werken met persoonsgegevens van slachtoffers, thuis en onderweg’.
- Je mag persoonsgegevens van slachtoffers uitsluitend raadplegen als dit noodzakelijk is voor de hulpverlening en dienstverlening aan het slachtoffer, of voor een van de andere doeleinden waarvoor Slachtofferhulp Nederland persoonsgegevens verwerkt.
- Je mag geen gegevens wegschrijven op privé-apparatuur (hiermee bedoelen we apparatuur buiten het netwerk van Slachtofferhulp Nederland). Dit is in strijd met de geheimhoudingsplicht. Slachtofferhulp Nederland is anders bovendien niet in staat om passende (organisatorische) maatregelen te treffen, zoals een gecontroleerde back-up ervan maken.
- Gebruik van WhatsApp wordt sterk afgeraden vanwege de veiligheid van de gegevens. Dit is vastgelegd in het Telecombeleid. Als alternatief is Signal beschikbaar op de mobiele telefoons van Slachtofferhulp Nederland.

Gebruikersnamen, wachtwoorden en rechten

- Om informatiesystemen en gegevens te kunnen gebruiken, krijgt iedere medewerker een uniek user-ID en een bijbehorend wachtwoord. Bij gebruik van meerdere systemen kunnen daar andere wachtwoorden bijkomen. Het wachtwoord is strikt persoonlijk. Je mag dit wachtwoord niet doorgeven aan andere personen, ook niet aan collega’s.
- Wijzig wachtwoorden minimaal elke 45 dagen om misbruik te voorkomen.
- Vul je vijf keer een fout wachtwoord in, dan blokkeert het beveiligingssysteem automatisch het algemene gebruikersaccount. De ICT-Helpdesk kan je gebruikersaccount weer vrijgeven.

- Let bij het omgaan met wachtwoorden op het volgende:
  - Schrijf wachtwoorden nooit op.
  - Gebruik zogenaamde ‘sterke wachtwoorden’, dit houdt in:
    - Niet gemakkelijk te raden, bijvoorbeeld geen naam van partner, kind, huisdier.
    - Wel gemakkelijk te onthouden, bijvoorbeeld de eerste letters of de titel van het laatst gelezen boek + cijfers.
    - Minimaal 10 karakters, het liefst langer. Tip: gebruik een zin.
- 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 alleen een leidinggevende aanvragen, met toestemming van de systeemeigenaar (Slachtofferhulp Nederland). Voor vragen hierover je terecht bij de functioneel beheerder of, als deze niet bekend is, de ICT-Helpdesk.

Antivirus & Malware

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

- Gebruik uitsluitend programmatuur die Slachtofferhulp Nederland heeft geïnstalleerd.
- Zet de 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. Stuur ze door naar de ICT-Helpdesk en verwijder ze direct daarna.

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 de laatste werkzaamheden met het werkstation.
- Schakel het werkstation uit als deze aan het netwerk is gekoppeld.
- Laat niemand meer toe tot het werkstation.
- Neem direct contact op met de ICT-Helpdesk.
- 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, ook de antivirussoftware. Bij vragen kun je de ICT-Helpdesk e-mailen of bellen (0800 023 14 54).

E-mail en internetprotocol

Binnen Slachtofferhulp Nederland geldt een aantal regels voor het gebruik van e-mail en internet:

- Je mag e-mail en internet niet gebruiken voor doeleinden die in strijd zijn met de wet of met de kernwaarden van Slachtofferhulp Nederland, of die tegengesteld zijn aan de belangen van Slachtofferhulp Nederland. Beperkt persoonlijk gebruik van e-mail en internet is wel toegestaan, mits dit niet storend is voor de dagelijkse werkzaamheden.
- Je mag geen informatie verzenden, op eigen initiatief ontvangen of opslaan 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.
- Je mag niet anoniem of onder een fictieve naam berichten verzenden. Ook mag je niet zonder toestemming van Slachtofferhulp Nederland gebruikmaken van middelen om informatie te beveiligen zonder dat Slachtofferhulp Nederland in staat is kennis te nemen van de inhoud van het bericht.
- Materialen met auteursrecht kopiëren, wijzigen, verzenden of opslaan is alleen toegestaan met toestemming van de eigenaar van het auteursrecht.
- Je mag niet online gokken of kettingbrieven versturen.
- Programmatuur installeren op middelen van Slachtofferhulp Nederland is alleen toegestaan met toestemming van Informatievoorziening. Zo voorkomen we dat systemen van Slachtofferhulp Nederland met virussen of malware wordt besmet of dat de integriteit van de werkplek wordt geschonden.
- Je mag via het e-mailsysteem van Slachtofferhulp Nederland geen ‘algemene berichten’ met commerciële strekking verzenden die niet ten behoeve van het zakelijk verkeer zijn.
- Je mag niet zonder toestemming e-mailberichten van andere gebruikers openen.
- Vertrouwelijke of gevoelige bedrijfsspecifieke informatie verstrekken mag alleen in overleg met je leidinggevende.
- Je mag niet zo met toegangsgegevens omgaan dat je daarmee onbevoegden stimuleert om toegang te krijgen tot het netwerk van Slachtofferhulp Nederland.
- Voor het registreren, verzamelen, controleren, combineren of bewerken van informatie moet je de privacyreglementen van Slachtofferhulp Nederland in acht nemen.

Vanwege het privékarakter van de e-mailberichten van de medewerker en het recht op privacy kan Slachtofferhulp Nederland zich slechts in uitzonderlijke gevallen toegang verschaffen tot de mailbox van een medewerker. Slachtofferhulp Nederland kan dit alleen indien:

- Een medewerker hiervan op de hoogte is of zou kunnen zijn.
- Slachtofferhulp Nederland een gerechtvaardigd belang heeft om e-mails in te zien dan wel te controleren.
- Er is voldaan aan de proportionaliteiteis.

Onder uitzonderlijke gevallen valt een vermoeden van een strafbaar feit en ziekte van de werknemer die langer dan twee weken duurt, contact door de leidinggevende met de werknemer niet mogelijk is en ook de medewerker zelf vooraf bij vertrek geen maatregelen heeft genomen om met betrekking tot de werkzaamheden voortgang te laten plaatsvinden. De direct leidinggevende geeft de opdracht tot de toegang van de mailbox. In dringende situaties waarin de twee weken niet afgewacht kunnen worden, kan de opdracht eerder verstrekt worden.
Bij geplande afwezigheid is de medewerker verantwoordelijk voor het instellen van een afwezigheidsmelder. De medewerker zorgt in overleg met de leidinggevende voor een overdracht. Dit kan bijvoorbeeld door iemand te machtigen voor de mailbox.

Slachtofferhulp Nederland heeft de bevoegdheid om het e-mail- en internetgebruik van medewerkers zo nodig te monitoren en te controleren. Bij generieke controles zal dit in beginsel alleen plaatsvinden op het niveau van getotaliseerde gegevens die niet herleidbaar zijn tot identificeerbare personen. Indien er aanleiding is om specifiek onderzoek te verrichten zal dit alleen gebeuren in overleg met de Functionaris Gegevensbescherming en met toestemming van het hoofd HRM. De Voorzitter van de Raad van Bestuur wordt daarover geïnformeerd. Bij controle conformeert Slachtofferhulp Nederland zich aan de voorwaarden die voortvloeien uit de privacywetgeving te weten:

- *Redelijke verdenking*
  Slachtofferhulp Nederland heeft een redelijke verdenking dat een of meerdere werknemer(s) iets doen wat strafbaar of verboden is.
- *Kan niet anders*
  Het lukt Slachtofferhulp Nederland niet, ondanks gerichte inspanning, een eind te maken aan een mogelijk strafbaar feit. Dus het kan echt niet anders dan een of meer medewerker(s) heimelijk te controleren.
- *Incidenteel*
  De heimelijke controle is incidenteel. Dat betekent dat Slachtofferhulp Nederland de heimelijke controle alleen mag uitvoeren in een vooraf bepaalde periode.
- *Informeren*
  Slachtofferhulp Nederland informeert de betrokken medewerker(s) achteraf over de heimelijke controle. Ook als de controle niet heeft uitgewezen dat de verdenking terecht was.

Printen/documenten opslaan

Slachtofferhulp Nederland is verplicht de persoonsgegevens van haar cliënten en medewerkers te waarborgen. Je mag niet zonder toestemming van Slachtofferhulp Nederland 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 CRM (CRIS of SiBiS) 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 door Slachtofferhulp Nederland goedgekeurde draagbare media, zoals encrypted usb-sticks of een encrypted harddisk.
Als je (bijvoorbeeld bij thuiswerk) privacygevoelige gegevens via privé-ICT-middelen in de openbaarheid brengt, ben je zelf verantwoordelijkheid voor verlies, diefstal of onrechtmatige raadpleging door derden.

Melden van beveiligingsincidenten en verlies of diefstal

Iedere medewerker is verantwoordelijk voor het zo tijdig mogelijk melden van incidenten en zwakke plekken in de beveiliging van informatie. Je moet dit melden aan het Servicepunt of de afdeling Informatievoorziening, en aan je direct leidinggevende. Als in bruikleen gegeven apparatuur wordt gestolen of vermist, moet je dit ook direct doorgeven aan je leidinggevende en aan de afdeling Informatievoorziening of Servicepunt. Zo kunnen zij passende maatregelen nemen. Je moet bovendien aangifte doen.

Je bent zelf verantwoordelijk en aansprakelijk als (bijvoorbeeld bij thuiswerk) privacygevoelige gegevens via ICT-middelen in de openbaarheid worden gebracht. Bij gebruik van privémiddelen, moeten deze zijn voorzien van een actuele virusscanner. Ook moeten ze up-to-date zijn met alle (beveiligings-) updates van Microsoft, Apple en/of Android.
Als er privédata op je privé-device staan, valt de back-up onder je eigen verantwoordelijkheid.

Beheer ICT gebruiksreglement

De afdeling Informatievoorziening van Slachtofferhulp Nederland onderhoudt het ICT-gebruiksreglement.

Gebruikte definities

Bedrijfsmiddelen	ICT-middelen en overige middelen die Slachtofferhulp Nederland beschikbaar stelt om de functie te kunnen uitoefenen.
ICT-middelen	Apparatuur, programmatuur, licenties.
CRM	Cliënt Relatie Systeem, ofwel CRIS of SiBiS.
Apparatuur	Werkstations, printers, beamer, mobiele en vaste telefoons.
Werkstations	Thin Clients, mobiele Thin Clients, desktops en laptops.
Mobiele devices	Mobiele telefoons en tablets.
Medewerker/werknemer	Beroepskracht, inhuurkracht, vrijwilliger of stagiair.

Landelijk kantoor:
Postbus 14208, 3508 SH Utrecht
Moeder Teresalaan 100, 3527 WB Utrecht
Telefoonnummer 088 - 746 07 46
Hulp 0900 - 0101 (gebruikelijke belkosten)
www.slachtofferhulp.nl

Slachtofferhulp Nederland
Vandaag verder