Gedragsregels en tips voor informatieveiligheid

De Hartekamp Groep heeft als zorgorganisatie de verplichting om persoonsgegevens van cliënten en medewerkers te beschermen. Deze verplichtingen vloeien voort uit de Algemene Verordening Gegevensbescherming of de Wet Cliëntenrechten bij elektronische verwerking van gegevens. Bescherming van persoonsgegevens geldt ook vanuit zorgwetten zoals Wmo, Jeugdwet, Wlz en Wgbo.

Deze wetten stellen eisen aan organisatorische en technische beveiligingsmaatregelen om de privacy van cliënten en medewerkers zeker te stellen. Dit betekent dat beschikbaarheid en betrouwbaarheid van de ICT-infrastructuur en kritische applicaties (ECD, ANW-omgeving) en behandeling van persoonsgegevens goed geregeld moeten zijn.

Minstens zo belangrijk is dat iedereen binnen de Hartekamp Groep bewust is van een veilige omgang met (persoons)gegevens en gebruik van bedrijfsmiddelen. We moeten ook beseffen dat je privé-omgeving belangrijk is; we gebruiken een privécomputer, tablet of smartphone ook voor zakelijke e-mails of andere applicaties. Tegelijkertijd gebruiken we bedrijfsmiddelen soms ook voor privédoeleinden. Werk en privé komen steeds dichter bij elkaar.

Om je in de werk- en privéomgeving te helpen zijn tien gedragsregels en bijbehorende ‘tips’ opgesteld:

1. Houd wachtwoorden geheim.
2. Behandel informatie met zorg.
3. Ga zorgvuldig om met telefoon, e-mail en internet.
4. Let op bij het gebruik van mobiele apparatuur.
5. Ken het risico van externe gegevensdragers.
6. Geef aandacht aan fysieke beveiliging.
7. Gebruik alleen geautoriseerde hardware en software.
8. Respecteer de wet, je contract, het beleid en de gedragsregels.
9. Weet met wie je contact hebt.
10. Meld diefstal en oneigenlijk gebruik.

Heb je vragen over hoe je het beste met vertrouwelijke (persoons)gegevens of ICT-voorzieningen om kunt gaan? Mail dan naar a.tiller@hartekampgroep.nl / security-privacy@hartekampgroep.nl of via 06 - 4624 5227.

Arnoud Tiller
Security & Privacy Officer en Functionaris Gegevensbescherming

1. Houd wachtwoorden geheim

Wachtwoorden worden gebruikt voor toegang tot werkstation, tablets, applicaties, accounts op internet, e-mail en andere (betaal)diensten. Maar hoe ga je om met de (pincode) bij tablets en mobiele telefoons? Deze kunnen tegenwoordig hetzelfde als computers… Het gebruik van mobiele telefoons, e.d. wordt in het onderwerp *'Ga zorgvuldig om met telefoons, e-mail en internet' behandeld*.

Wachtwoorden (en dus ook pincodes) zijn geliefd bij criminelen. Zijn die bekend, dan kunnen criminele activiteiten uitgevoerd worden zoals het plaatsen van schadelijke – en 'afluister' software op ons ICT-netwerk, computer, tablet of mobiele telefoon. Een sterk wachtwoord en veilig gebruik is dus belangrijk. *Natuurlijk worden persoonsgegevens (cliënten/medewerkers) niet op privémiddelen gebruikt.*

Hoe krijg je veilig een veilig wachtwoord?
De belangrijkste stappen zijn:

- Wachtwoorden niet toegankelijk voor anderen.
- Maak sterke wachtwoorden op basis van een wachtwoordzin.
- Gebruik overal een ander wachtwoord.
- Gebruik een wachtwoordmanager.

Wachtwoorden niet toegankelijk voor anderen
Bij Internet Explorer, Google Chrome, Firefox en Safari wordt gevraagd of je wachtwoorden wilt laten onthouden; handig, maar onveilig! Wachtwoorden zijn makkelijk te achterhalen als je computer tablet of mobiele telefoon niet goed is vergrendeld of geen sterk wachtwoord heeft.

Maak een sterk wachtwoord
Hoe langer een wachtwoord, hoe moeilijker deze is te raden, hacken. Een woord, cijferreeks of een combinatie (Welkom123) is door een computerprogramma die hackers inzetten, snel geraden. In de video 'Hoe kraakt iemand een wachtwoord' wordt dit op een eenvoudige manier uitgelegd.

Gebruik een basiswachtwoord
In de digitale wereld heb je genoeg aan twee aparte basiswachtwoorden voor werk en privé. We werken dit voor het werk uit in vier stappen:

1. Kies een zin die makkelijk is te onthouden. Bijvoorbeeld *'Het is fijn om met applicatie X te werken!*'.
2. Gebruik de eerste letter van elk woord. Het wachtwoord is nu: *HifomaXtw!*
3. Vervang één of meerder (mede)medeklinkers in het wachtwoord. In ons voorbeeld wordt de letter o vervangen door het cijfer 9 en de letter a door het cijfer 1. Het wachtwoord is dan: *Hif9m1Xtw!*
4. Moet je wachtwoord gewijzigd worden dan kan je bijv. het laatste cijfer veranderen. Je krijgt dan *Hif9m**2**Xtw!* als nieuw wachtwoord. Natuurlijk kan je ook een ander karakter wijzigen.

Gebruik overal een ander wachtwoord
Als je wachtwoord ergens wordt gehackt, dan moet je deze overal wijzigingen. Alleen op deze manier kan er geen misbruik worden gemaakt van je persoonsgegevens. Voeg daarom voor elke website iets unieks toe aan het basiswachtwoord.

In dit voorbeeld is het basiswachtwoord uit de wachtwoordzin: *Hif7md3Xtw!* Bedenk een kort zinnetje waar ook weer de eerste letter van elk woord wordt gebruikt. Bijvoorbeeld 'Gmail is handig' of 'Facebook is gezellig'. Bij Gmail wordt het wachtwoord *Hif7md3Xtw!Gih* en het wachtwoord *Hif7md3Xtw!Fig* gebruik je bij Facebook.

Gebruik een wachtwoordmanager
Dit is handig; wachtwoorden bewaren en bijhouden in een veilige kluis! Bij de eerste keer inloggen op een website vraagt het programma of het de gegevens moet onthouden. Doe je dat, dan worden ze voortaan automatisch ingevuld. Een wachtwoordmanager kan gebruikt worden op computer, tablet en mobiele telefoon.

Enkele bekende wachtwoordmanagers zijn LastPass, 1Password, DashLane, KeePass, Roboform en de managers van F-Secure Key, Intel True Key, Kaspersky Password Manager en Norton Identity Safe. Om een goed beeld te krijgen welke wachtwoordmanager het beste bij je past kan je op internet diverse vergelijkende onderzoeken raadplegen.

2. Behandel informatie met zorg

Werk je regelmatig of elke dag met persoonsgegevens van cliënten of collega's, financiële of andere vertrouwelijke informatie van de Hartekamp Groep? Stel jezelf dan regelmatig de vraag: *"Hoe wil ik dat mijn bank, verzekeringsmaatschappij, ziekenhuis of dokter met mijn persoonlijke gegevens omgaat?"*

We werken dagelijks met programma's zoals ECD of Youforce, Coda maar ook met papieren documenten. De Hartekamp Groep moet voldoen aan uiteenlopende privacywetten. Ook cliënten en medewerkers vertrouwen erop dat we hun (persoons)gegevens op een veilige manier behandelen. Je kan hier zelf aan bijdragen door eenvoudige handelingen uit te voeren:

- Weet zeker dat je vertrouwelijke (persoons)gegevens verstrekt aan medewerkers, externe organisaties die een, relevante, zakelijke relatie hebben met de Hartekamp Groep.
  We doen dit in veel gevallen per e-mail, dus verifieer of je het goede e-mailadres gebruikt. Zorg dat je bij het versturen van vertrouwelijke gegevens gebruikt maakt van Zorgmail (aanwezig binnen onze organisatie) of dat het bestand is beveiligd met 7-Zip. Vanuit privacywetgeving is dit is verplicht.
- Geef alleen informatie (in zakelijk verband) aan medewerkers, externe organisaties die ter zake doet. Het toesturen van een rapportage in Word of PDF is handig maar vaak bevat dit ook informatie die niet gedeeld hoeft te worden. Vanuit privacywetgeving is dit ook niet toegestaan!
- Laat geen informatie over cliënten, medewerkers en de Hartekamp Groep onbeheerd op en rond je bureau of kantoorruimte liggen.
- Laat geen vertrouwelijke informatie achter in gemeenschappelijke ruimten. Verwijder na gebruik vertrouwelijke informatie van Whiteboards en flip-overs.

- Haal print- en kopieerwerk direct van het betreffende apparaat en vergeet de originelen niet mee te nemen. In de praktijk blijkt dat bij onbeveiligde printers, veelvuldig medische rapportages, sollicitatiebrieven met cv's en andere documenten liggen.
- Gooi papieren met vertrouwelijke informatie niet in de prullenbak, maar gebruik een papiervernietiger of deponeer ze in de blauwe papiercontainers.
- Zorg dat externe (kostbare) informatiedragers (laptop, tablet , USB-stick, etc.) na gebruik worden opgeborgen in een afsluitbaar opbergsysteem.
- Als externe gegevensdragers niet meer gebruikt worden dan moet de informatie op een veilige manier permanent worden weggehaald. Vraag om meer informatie bij ICT Servicedesk.
- Binnen de Hartekamp Groep, 'vergrendelen' werkstations zich na enige minuten van inactiviteit automatisch. Handig, maar vergrendel altijd je werkstation bij het (tijdelijk) verlaten van je werkplek en/ of kantoorruimte. Hiermee voorkom je dat iemand (privé)mail, werkdocument leest of toegang tot persoonsgegevens krijgt via een applicatie.
- Bespreek geen vertrouwelijke informatie binnen gehoorafstand van derden.
- Het is voor derden vrij eenvoudig om via gratis, open Wifi-punten je handelingen te volgen… Maak als je een laptop, tablet of smartphone voor (zakelijke) werkzaamheden geen gebruik van gratis, open Wifi-punten. Gebruik je smartphone als 'tijdelijke hotspot' (instellingen > hotspot) zodat je een eigen, beveiligde verbinding hebt.
- Attendeer je collega('s) op onveilig gedrag en leg uit waarom dit zo is.

3. Ga zorgvuldig om met telefoon, e-mail en internet

De door de Hartekamp Groep verstrekte communicatiemiddelen, zoals (mobiele) telefoon, e-mail en internet, zijn primair bestemd voor zakelijk gebruik. Soms gebruiken we deze middelen ook privé om wat op te zoeken en te bellen; beperk dit dan tot een minimum en in beide situaties gelden wel gedragsregels. Lees ook eens de *'Richtlijn voor het gebruik van social media'* die op Infoland staat.

Vanuit informatieveiligheid en privacybescherming voor onze cliënten en medewerkers gelden de volgende gedragsregels:

- Veel communicatie en het delen van vertrouwelijke (persoons)gegevens gebeurt via e-mail. Hierdoor is het risico ook groter dat er incidenten kunnen plaatsvinden. Verstuur vertrouwelijke (persoons)gegevens met alleen via daarvoor bestemde voorzieningen van de Hartekamp Groep (ZorgMail of een beveiligde bijlage). Gebruik je zakelijke e-mail op je privé smartphone? Dit is niet toegestaan tenzij je voldoet aan de beveiligingseisen voor smartphones van de Hartekamp Groep.
- Stel je zelf vragen als; moet ik dit document toesturen of is een gedeelte ook voldoende? En ook aan deze collega's of instantie?
- Controleer of ontvangen e-mails van betrouwbare of bekende e-mail adressen zijn.
- Vertrouw je een email niet? Check of de mail op de lijst van bekende Phishing mails bij een bedrijf staat als KPN, Ziggo, e.d. Is dit niet het geval? Stuur hem dan door naar de ICT-Servicedesk.

- Gebruik alleen betrouwbare apps; Apps verzamelen vaak meer gegevens dan we ons realiseren. Dit geldt met name voor apps die buiten de officiële app-stores worden aangeboden. Het risico op malware is bij deze apps een stuk groter... Gebruik je een Ons-App, e.d. met vertrouwelijke (persoons)gegevens op je privételefoon? Dit is niet toegestaan tenzij je voldoet aan de beveiligingseisen voor smartphones van de Hartekamp Groep.
- Gebruik een goede pincode (en nog liever; sterke wachtwoorden en / of biometrische beveiliging) op je telefoon. Het is slim om een willekeurige vier- (en bij voorkeur zes-) cijferige combinatie te gebruiken. Dus geen 111111, 12121212, 123456 of geboortedatum. Gebruik een datum die voor jou bijzonder en vrij onbekend is; huwelijksdatum, geboortedatum kinderen, e.d. Biometrische beveiliging, zoals vingerafdrukscanner, werken op basis van persoonskenmerken waardoor een hoog beveiligingsniveau ontstaat. Veel telefoons zijn tegenwoordig uitgerust met deze beveiliging.
- Maak (zo min mogelijk) gebruik van openbare wifi-netwerken; vaak ontbreken een goede beveiliging en versleuteling van de data. Cybercriminelen gebruiken dit soort wifi-verbindingen om data te onderscheppen, uit te lezen en te misbruiken. Gebruik dus vertrouwde wifi-netwerken of mobiele 3G/4G-dataverbindingen.
- Het benaderen, downloaden of verzenden van illegaal, aanstootgevend materiaal is niet toegestaan. Binnen de Hartekamp Groep zijn en worden maatregelen getroffen om dit zoveel mogelijk te blokkeren.

4. Let op bij het gebruik van mobiele apparatuur

Mobiele apparaten (zoals laptops, tablets en smartphones) zijn klein, licht en gemakkelijk overal mee naar toe te nemen. Het zijn gebruiksvoorwerpen waar we bestanden met (persoons)gegevens op plaatsen en mee versturen. Maar mobiele apparatuur is ook kwetsbaar (hackers, virussen, e.d.) en diefstalgevoelig. Ze vormen daardoor een risico en extra bescherming is nodig.

Hieronder volgen de belangrijkste tips voor het veilig gebruik van mobiele apparatuur:

- Zorg dat door de Hartekamp Groep verplicht gestelde beveiligingssoftware is geïnstalleerd. Met deze software is het mogelijk om gegevens te versleutelen en bij diefstal op afstand te wissen.
- Bescherm je mobiele apparatuur altijd met een sterk wachtwoord, pincode of indien mogelijk met biometrische beveiliging (zoals vingerafdrukscanner).
- Houd je mobiele apparatuur zorgvuldig bij je en laat deze nooit onbeheerd achter
- Zorg ervoor dat niemand mee kan kijken of luisteren als je met vertrouwelijke informatie werkt.
- Vergrendel na gebruik je (mobiele) apparatuur of sluit deze af zodat misbruik niet mogelijk is (clear-screen).
- Bewaar en vervoer mobiele apparatuur op een niet zichtbare plaats.
- Gebruik voor je apparatuur geschikte beschermingsmiddelen om fysieke schade te voorkomen.

- Zorg dat je in geval van schade of diefstal dit zo spoedig mogelijk (< 24 uur) meldt bij de ICT Servicedesk. De ICT Servicedesk kan dan met behulp van de beveiligingssoftware de zakelijke (persoons)gegevens op afstand van je apparatuur verwijderen.
- Bij reparatie of verkoop van een (mobiel) apparaat moet de ICT Servicedesk altijd eerst de zakelijke (persoons)gegevens op een veilige manier wissen.

5. Ken het risico van externe gegevensdragers

Externe gegevensdragers (USB, externe harde schijf, Cd-rom, e.d.) zijn klein, licht en gemakkelijk mee te nemen. Handig voor het geven van een presentatie. Of om (media) bestanden met vertrouwelijke (persoons)gegevens tijdelijk op te slaan. De kans op verlies, vergeten of het (onbedoeld) geïnfecteerd zijn met schadelijke software is aanwezig en zorgvuldige, veilige omgang is nodig.

Hieronder enkele tips voor het veilig gebruik van externe gegevensdragers:

- Gebruik externe gegevensdragers als dit echt nodig is en laat ze niet onbeheerd achter.
- Verwijder direct bestanden, documenten als je deze niet meer nodig hebt*. Voor een gemiddelde derde is dit voldoende maar wist je dat na het verwijderen of 'formatteren' de gegevens nog op de gegevensdrager staan? Test dit eens met het gratis programma Piriform Recuva. Stel je voor dat een kopie van een paspoort, ID-bewijs of andere vertrouwelijke (persoons)gegevens nog steeds aanwezig is? Voor volledige verwijdering kan je ook het softwarepakket CCleaner gebruiken.*
- Bewaar externe gegevensdragers in een afgesloten kast of kluis en vervoer deze niet op een zichtbare plaats.
- Voer altijd een viruscontrole uit op de externe gegevensdrager als je deze hebt gebruikt buiten de vertrouwde ICT-omgeving van de Hartekamp Groep. Het is mogelijk dat (onbedoeld) de gegevensdrager is geïnfecteerd met schadelijke software.
- Voer altijd een viruscontrole uit op de externe gegevensdrager als je een bestand plaatst dat afkomstig is van buiten de vertrouwde ICT-omgeving van de Hartekamp Groep. Het is mogelijk dat (onbedoeld) de gegevensdrager is geïnfecteerd met schadelijke software.

6. Geef aandacht aan fysieke beveiliging

Kunnen onbekenden zomaar in je huis rondlopen? Laat je voor- en achterdeuren en ramen open als je weggaat? Zijn je bankafschriften, verzekeringspolissen en andere persoonsgegevens voor bezoekers te zien? Waarschijnlijk niet; je wilt voorkomen dat anderen bezittingen meenemen of privégegevens kunnen lezen. Hetzelfde geldt voor de Hartekamp Groep; we willen niet dat bedrijfsmiddelen en vertrouwelijke (persoons)gegevens van onze cliënten, medewerkers of organisatie in handen komen van kwaadwillende derden.

Hieronder enkele aandachtspunten om gebouwen, bedrijfsmiddelen en (persoons)gegevens van veilig te stellen:

- Leen je (Salto)toegangspas niet uit aan collega's of derden; het is aan jou in bruikleen gegeven en je bent hiervoor persoonlijk verantwoordelijk.

- Controleer of beveiligde (buiten)deuren in het slot vallen en blokkeer de beveiliging niet. Zorg voor toezicht als een buitendeur van een bouwwerk vanwege werkzaamheden tijdelijk open moet blijven.
- Haal bezoeker(s) op uit de hal of bij de voordeur en begeleid deze bij vertrek naar de buitendeur.
- Spreek (binnentredende) bezoekers vriendelijk aan en vraag met welke collega een afspraak is gemaakt. Als de collega (nog) niet aanwezig is, bel deze dan of breng de bezoeker naar de betreffende collega. Laat een bezoeker niet alleen achter zonder verificatie over zijn / haar aanwezigheid. Een bezoeker ervaart een persoonlijke begroeting en begeleiding als een hartelijk welkom, professioneel en zeker niet als storend.
- Laat vertrouwelijke (persoons)gegevens over cliënten, medewerkers en de Hartekamp Groep niet onbeheerd op, en rond je bureau of kantoorruimte liggen (clean desk).
- Vertrouwelijke (persoons)gegevens zijn na kantoortijd in afsluitbare (lade)kasten of bureaus opgeborgen (clean desk).
- Laat geen vertrouwelijke (persoons)gegevens achter in gemeenschappelijke ruimten. Verwijder na gebruik vertrouwelijke gegevens van Whiteboards, flip-overs, e.d..
- Laat bedrijfsmiddelen (zoals laptop, tablet en telefoon) niet onbeheerd achter in je auto of tijdens vervoer buiten het bedrijfspand. Dit geldt ook voor fysieke dossiers met vertrouwelijke (persoons)gegevens.
- Deponeer papieren documenten met vertrouwelijke (persoons)gegevens in de bekende, afgesloten blauwe bakken of versnipper de documenten.
- Meld ‘vreemde’ situaties van onbekende personen of onvoldoende functionerende beveiligingsmaatregelen direct aan je leidinggevende, TTV’er Facilitair of Veiligheid of afdeling Vastgoed.

7. Gebruik alleen geautoriseerde hardware en software

We willen allemaal dat een PC, laptop, tablet en smartphone betrouwbaar is, altijd functioneert en er op een veilige manier mee gewerkt kan worden. Het zelf wijzigingen van instellingen of installeren, van hard- en software kan negatieve invloed hebben op prestaties. Vooral het downloaden en installeren van software die niet afkomstig is van vertrouwde, bekende aanbieders / stores leidt tot onnodige risico’s. Dit kan je voorkomen door de volgende regels toe te passen:

- Wijzig nooit de instellingen van je zakelijke werkstation, laptop, tablet of smartphone.
- Het is niet toegestaan om op door de Hartekamp Groep ter beschikking gestelde bedrijfsmiddelen zelf software te installeren. Op het Internet staat ogenschijnlijke interessante software die na installatie, de instellingen veranderen of kwaadaardige software bevatten.
- Het is niet toegestaan illegale kopieën van software te gebruiken op door Hartekamp Groep ter beschikking gestelde bedrijfsmiddelen.
- Sluit geen eigen / onbekende hardware, externe gegevensdragers aan op het bedrijfsnetwerk en wijzig nooit instellingen van randapparatuur.

- De Hartekamp Groep verstrekt beveiligde bedrijfsmiddelen als je vanuit je functie buiten de kantooromgeving of thuis werkzaamheden uitvoert. Als je onverhoopt je eigen apparaten gebruikt voor zakelijke doeleinden, zorg dan voor een gedegen en up-to-date virusscanner en firewall, ingesteld op het hoogste veiligheidsniveau op je eigen apparaten.
- Vraag bij twijfel altijd om advies of hulp van de ICT Servicedesk.

8. Respecteer de wet, je contract, het beleid en de gedragsregels

De Hartekamp Groep moet voldoen aan uiteenlopende wetten, afspraken met zorg-ketenpartners en verplichtingen naar cliënten, medewerkers, vrijwilligers, stagiaires en derden. Het hieraan niet voldoen kan leiden tot risico's voor de organisatie. Om deze verplichtingen allemaal in goede banen te leiden is dit vastgelegd in beleid, protocollen, gedragsregels en in contracten met externe partijen en werknemers.

- Respecteer privacywetgeving zoals de Algemene Verordening Gegevensbescherming en specifieke zorgwetten en het portretrecht vanuit de Wet Auteursrecht. Op basis hiervan moet de Hartekamp Groep kostbare investeringen doen om informatie te beveiligingen.
- Houd je aan de gedragsregels en privacybeleid van de Hartekamp Groep.
- Houd je aan het arbeidscontract en de geheimhoudingsplicht die je hebt afgesproken.
- Houd je aan het beleid voor informatiebeveiliging en andere instructies en richtlijnen op dit vlak.
- Raadpleeg bij twijfel je leidinggevende of vakinhoudelijke collega.

9. Weet met wie je contact hebt

Het is iedereen wel eens gebeurd; een onbestemd gevoel of de omgeving, situatie en persoon juist was om vertrouwelijke (persoons)gegevens te bespreken of te verstrekken. Hoe kan je dit voorkomen? Vertrouw je morele kompas en besef dat het bespreken van vertrouwelijke (persoons)gegevens in publieke omgevingen ongewenst en niet professioneel overkomt naar anderen. Enkele simpele en logische tips om je te helpen zijn:

- Verstrek telefonisch of per e-mail geen (persoons)gegevens aan onbekenden. Als je twijfelt, reageer op een later tijdstip en verifieer of je met de juiste persoon of instantie contact hebt.
- Vraag om terug te bellen als er geen geschikte besloten ruimte is om je gesprek te voeren.
- Geef alleen (persoons)gegevens die ter zake zijn om een vraag te beantwoorden. Stel jezelf dus de vraag of het echt nodig is om meer gegevens te verstrekken dan strikt nodig is. Gemakzucht leidt tot onveiligheid…

- Om te voorkomen dat teveel personen informatie over een cliënt krijgen, beperk je de communicatie zoveel mogelijk tot één contactpersoon.
- Iedereen in een openbare ruimte kan meeluisteren met jouw gesprek. Denk daaraan voordat je vertrouwelijke gegevens gaat delen.
- Bij iedere handeling met een cliënt, staat de veiligheid van een cliënt voorop: dat geldt ook voor de schriftelijke communicatie over de cliënt met anderen. Natuurlijk doe je dat via veilig mailen met ZorgMail van de Hartekamp Groep.

10. Meld diefstal en oneigenlijk gebruik

Ondanks alle voorzorgmaatregelen zijn incidenten niet altijd te voorkomen. Meld het direct als je een onveilige situatie tegenkomt! Door een snelle melding kunnen we passende maatrelen treffen. Het verliezen van je toegangspas of bedrijfsmiddel, het onveilig digitaal versturen van persoonsgegevens of bezoekers die niet begeleid worden, zijn voorbeelden van incidenten. Maar ook gevoelige informatie die in een overlegruimte achtergebleven is, kan een melding waard zijn.

- Je bent als medewerker van de Hartekamp Groep verplicht om beveiligingsincidenten en beveiligingslekken te melden; deze worden altijd vertrouwelijk behandeld.
- Incidenten met betrekking tot fysieke beveiliging moet je onmiddellijk melden bij de Front-Office.
- Als je Saltopas kwijt is moet je dit onmiddellijk melden bij de Front-Office of ICT Servicedesk.
- Als de laptop, tablet of mobiele telefoon die je van de Hartekamp Groep hebt gekregen, is gestolen of kwijtgeraakt, moet je dit onmiddellijk melden bij ICT Servicedesk. Deze kunnen op afstand, met behulp van de geïnstalleerde beveiligingssoftware, de apparatuur blokkeren en aanwezige gegevens verwijderen.
- Incidenten met betrekking tot informatiebeveiliging meld je per FOBO-melding of e-mail bij de Security & Privacy Officer.
- Bij diefstal moet binnen 24 uur aangifte worden gedaan bij de Politie en dient de verantwoordelijke afdeling binnen de Hartekamp Groep geïnformeerd zijn.