# Procedure toegang en beveiliging

| Beheerder | Rien Romijn |
|---|---|

Binnen Romijn & Lenders Assurantiën is het belangrijk dat privacy wordt bewaakt en informatie niet in verkeerde handen terecht komt. Daarom zijn er binnen ons kantoor verschillende maatregelen getroffen. Eenieder is verantwoordelijk voor alle aspecten van informatiebeveiliging in de eigen invloedssfeer.

1. De directie heeft passende technische en organisatorische maatregelen getroffen om persoonsgegevens te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking. Hiertoe zijn verschillende gedragscodes, beveiligingsrichtlijnen en procedures opgesteld waar eenieder zich aan dient te houden.

2. Binnen ons kantoor is informatiebeveiliging contractueel uitbesteed aan Cremers Computer Company.

**Organisatorische beveiliging**

3. Eenieder zijn verplicht vertrouwelijk om te gaan met persoonlijke en financiële gegevens van de klant, voor hen geldt een zwijgplicht over deze (financiële) gegevens.

4. Eenieder binnen ons kantoor krijgt een eigen inlognaam en wachtwoord om in te loggen op het systeem. Daarnaast worden er logbestanden bijgehouden waarin toegang op individueel niveau wordt vastgelegd. Dat maakt het mogelijk om misbruik van toegang achteraf vast te stellen.

5. Het is alleen toegestaan om gebruik te maken van USB-sticks, externe harde schijven etc. voor opslag van persoonsgegevens indien er geen enkele andere mogelijkheid is voor opslag. Indien een medewerker gebruik maakt van deze devices zal dit uitsluitend in overleg met de directie plaatsvinden.

6. De directie heeft bepaald dat binnen ons kantoor uitsluitend wordt gewerkt met originele hardware en software. De directie heeft bepaald dat beschikbare updates altijd direct moeten worden geïnstalleerd. Cremers Computer Company is hiervoor verantwoordelijk.

7. Het niet toegestaan om zelf, zonder toestemming van de directie, hardware en/of software te installeren binnen ons kantoor. Eveneens is het medewerkers niet toegestaan om via eigen devices mobiel te werken (denk bijvoorbeeld aan email).

**Fysieke beveiliging**

8. Medewerkers, bezoekers en leveranciers hebben uitsluitend toegang te hebben tot ruimtes waar zij moeten zijn. Daarom zijn er fysieke beveiligingsmaatregelen getroffen, zoals toegangsrechten tot het geboruw. De serverruimte mag niet onbeheerd worden achtergelaten. Als er niemand meer in de ruimte aanwezig is, dient deze altijd afgesloten te zijn.

9. Binnen ons kantoor hebben directie en de medewerker toegang tot de serverruimte.

**Backups en updates**

10. De directie heeft bepaald dat er dagelijks twee back ups worden gemaakt van alle systemen welke persoonsgegevens bevatten. Deze back up wordt:
    a. Lokaal gemaakt en bewaard op een externe locatie.
    b. Extern gemaakt en wordt op één locatie in Nederland opgeslagen.
    c. Het is op dit moment niet bekend of de backups encrypted zijn.

11. Bij iedere backup wordt gecontroleerd of deze succesvol is verlopen, zodat er geen persoonsgegevens verloren kunnen gaan.

12. Periodiek worden backups teruggezet om te controleren of het backup proces voldoet en borgt dat persoonsgegevens niet verloren gaan.

**Toegang tot systemen**

13. Eenieder op ons kantoor heeft de rechten tot inzage van klantdossiers op alle niveau's.

14. Personeelsdossiers zijn alleen toegankelijk voor directie.

15. Computers zijn op dit moment nog niet zodanig ingesteld dat er na een bepaalde inactieve periode opnieuw moeten worden ingelogd.

16. Eenieder is zelfstandig verantwoordelijk voor het feit dat wachtwoorden en inloggegevens niet met collega's of derden worden gedeeld. Bij misbruik van deze gegevens zal de medewerker hiervoor verantwoordelijk worden gehouden.

17. Binnen ons kantoor:
    a. Moet worden ingelogd met een persoonlijk wachtwoord op de computer.
    b. Moet voor beschikbare applicaties apart worden ingelogd.
    c. Daarbij wordt zoveel mogelijk gebruik gemaakt van een digitaal paspoort.

18. Eenieder is verplicht om standaardwachtwoorden direct na ontvangst van nieuwe hardware en/of software te wijzigen.

19. Een wachtwoord moet driemaandelijks worden aangepast en voldoen aan onderstaande factoren:
    a. Minimaal 8 tekens
    b. Bevat minimaal 1 cijfer
    c. Bevat minimaal 1 leesteken

20. De directie van ons kantoor controleert op steekproefsgewijze basis of wachtwoorden worden aangepast.

**Bescherming van gegevens**

21. Binnen ons kantoor is op alle computers en servers antivirussoftware en firewalls geïnstalleerd en dagelijks wordt gecontroleerd of deze software werkt en actueel is.

22. De directie heeft bepaald dat Cremers Computer Company ervoor moet zorgdragen dat binnen het kantoor altijd de laatste versies van antivirussoftware en firewalls op de computers en servers zijn geïnstalleerd.

**Verwerkers**

23. Door ons kantoor wordt samengewerkt met externe partijen voor het verwerken van de (persoons)gegevens die wij verwerken. Deze samenwerking bestaat uit:
    a. Online advies-, vergelijkings-, administratie- of planningssoftware.
    b. Online backup faciliteiten

24. Met deze verwerkers zijn schriftelijke afspraken gemaakt welke zijn vastgelegd in een verwerkersovereenkomst. Dit om de (persoons)gegevens waarvan de verwerking door ons kantoor wordt uitbesteed te borgen.

**Wifi-netwerken**

25. De inloggegevens van ons bedrijfsnetwerk mogen nimmer worden verstrekt aan derden.

26. Het is niet toegestaan om met een zakelijk device contact te maken met een openbaar en onbeveiligd wifi-netwerk. Dit omdat dan niet geborgd kan worden dat derden zich geen toegang kunnen verschaffen tot de (persoons)gegevens die wij binnen ons kantoor verwerken.

**Vertrek personeel**

27. Bij het uit dienst treden van een medewerker wordt op basis van de checklist 'Personeel uit dienst' alle punten afgewikkeld om er zeker van te zijn dat de medewerker geen toegang meer heeft tot ons kantoor en de systemen.

**Website**

28. Op de website van ons kantoor kunnen klanten:
    a. Het contactformulier invullen
    b. Een verzekering aanvragen
    c. Inloggen in het digitaal klantdossier

<u>Bijlage:</u>
Checklist personeel uit dienst