Document:	Gedragscode voor Informatiebeveiliging
Vaststellingsdatum:	16-9-2025
Beoordelingscyclus:	16-9-2027
Verantwoordelijke:	Adviseur Informatiebeveiliging en Privacy

Inleiding

Informatiebeveiliging is, zeker in de huidige situatie waarin we te maken hebben met steeds meer bedreigingen van buitenaf (denk aan hacks), een belangrijk aandachtspunt. De afspraken die we hiermee vastleggen zijn bedoeld om een veilige en betrouwbare omgeving te creëren voor het beheer en de bescherming van informatie binnen SGL holding.

Wat doen we in het kader van informatiebeveiliging?

1. We beschermen gegevens en waarborgen de vertrouwelijkheid, integriteit en beschikbaarheid van alle informatie die door SGL holding wordt beheerd.
2. We werken aan het vergroten van het bewustzijn en kennis van medewerkers over informatiebeveiligingsrisico's.
3. We zorgen ervoor dat we beveiligingsincidenten en datalekken voorkomen.
4. We leven de relevante wet- en regelgeving met betrekking tot informatiebeveiliging na.

Afspraken: hoe werken wij?

Het is van belang dat iedereen binnen SGL holding weet welke afspraken we met elkaar hebben gemaakt om informatiebeveiliging binnen SGL holding te waarborgen. Het is namelijk een verantwoordelijkheid van ons allemaal. Als je deze afspraken volgt, help jij ook mee aan het waarborgen van de integriteit, vertrouwelijkheid en beschikbaarheid van onze informatie te waarborgen.

1. **Gebruik van IT-middelen:**
   - Gebruik bedrijfsapparatuur, zoals computers en mobiele apparaten, alleen voor werk gerelateerde taken.
   - Vermijd het downloaden van verdachte bestanden of het bezoeken van onveilige websites. Controleer hiervoor of het webadres begint met 'HTTPS://' en door te klikken op het hiervoor vermelde slotje zie je tot wanneer het certificaat geldig is.
   - Download alléén apps uit de officiële App store.
2. **Incidenten- en datalekkenbeheer:**
   - Wat is een beveiligingsincident? Denk aan: zonder toestemming van afdeling I&A geïnstalleerde software, rondslingerende laptops en telefoons, leesbaar genoteerde wachtwoorden etc.
     Meld beveiligingsincidenten meteen bij de I&A afdeling via Topdesk of via privacy@sgl-zorg.nl (voor Relim is dit: privacy@relim.nl).
   - Volg de procedure voor de melding van datalekken zoals beschreven in het Protocol datalekken.
     Wat is het verschil tussen een beveiligingsincident en een datalek?
     Een beveiligingsincident hoeft niet altijd te leiden tot verlies of openbaarmaking van gegevens zoals bijvoorbeeld een phishing aanval die tijdig wordt herkend.
     Bij een datalek gaan gegevens verloren of komen zij in verkeerde handen terecht. Een voorbeeld hiervan is een e-mail met vertrouwelijke gegevens die naar de verkeerde ontvanger wordt gestuurd.
   - Werk mee aan onderzoek naar beveiligingsincidenten en implementeer aanbevolen maatregelen om toekomstige incidenten te voorkomen.

3. **Training en Opleiding:**
    - Voor elke medewerker is er een e-learning Informatiebeveiliging en Privacy beschikbaar die je via Kompas/Leerplein/Algemene Verordening Gegevensbescherming (AVG) kunt maken. Omdat het om een dergelijk belangrijk onderwerp gaat is deze e-learning voor iedere medewerker verplicht om te maken.
    - Pas geleerde kennis en vaardigheden toe in de dagelijkse werkzaamheden.
    - We publiceren regelmatig tips, aandachtspunten en nieuwsbrieven over informatiebeveiliging op Kompas. Lees deze informatie zorgvuldig.
4. **Naleving en Sancties:**
    - We houden ons allemaal aan bovengenoemde afspraken voor de veiligheid van SGL holding als organisatie maar ook van jou als medewerker, cliënt, vrijwilliger en naaste.
    - Als je je bewust niet aan de afspraken houdt, dan kan SGL holding overgaan tot disciplinaire maatregelen, inclusief beëindiging van jouw dienstverband.
    - We voeren audits en controles uit om de naleving van deze afspraken te waarborgen.

Samen houden we SGL en Relim veilig.

Heb je daarover nog vragen? Stel ze gerust aan de Adviseur privacy en informatiebeveiliging, Wim Houben, mail naar whouben@sgl-relim.nl.