PGGM Informatiebeveiligingsregels

Het doel van dit document is de regels te geven waaraan elke interne en externe PGGM medewerker zich moet houden. Kom je in een situatie dat je je er niet aan kunt houden? Overleg dat dan met je manager en zoek samen met een oplossing. Vinden jullie geen oplossing bespreek het dan met collega's van IFS Service Point (9777). De informatiebeveiligingsregels worden onderhouden door de afdeling IFS/APC. IFS Service Point stelt de regels aan nieuwe medewerkers beschikbaar.

Toegang

Voor het gebouw, de lockers en de printers heb je een strikt persoonlijke toegangspas:

- Draag je toegangspas zichtbaar;
- Spreek een onbekende erop aan als deze zijn/haar pas niet zichtbaar draagt. Als je het niet vertrouwt, bel dan de beveiliging (9494);
- Laat geen andere personen naar binnen of buiten met je eigen toegangspas;
- Heb je je pas thuis laten liggen, dan kun je bij de beveiligingsloge een tijdelijke pas krijgen;
- Pas vergeten op je werkplek? Loop even terug om je pas op te halen;
- Werkt je pas niet bij de toegangspoortjes? Dan ben je waarschijnlijk te snel doorgelopen. Loop dan naar de beveiligingsloge of het IFS Servicepoint om je pas te laten controleren;
- Bij verlies of diefstal meld je dit direct bij het IFS Servicepoint (9777).

Begeleid bezoekers

Meld bezoekers van tevoren aan, laat ze de aan jou uitgereikte bezoekerspas zichtbaar dragen en begeleid ze altijd door het gebouw en naar de uitgang totdat de receptie of de bewaking de bezoekerspas weer heeft ingenomen. Breng een verdwaalde bezoeker terug naar de receptie.

Netwerk

Voor je virtuele pc op het netwerk heb je een account, bestaande uit een user-id, een wachtwoord en een token (Zie de Quick Reference Card). Je account is strikt persoonlijk en wordt daarom beveiligd met een wachtwoord en een token. Geef je wachtwoord nooit af en schrijf het nooit op. Laat ook je token niet onbeheerd achter.

Gebruik voor je werk andere wachtwoorden dan voor privé. Kies een niet gemakkelijk te raden maar wel gemakkelijk te onthouden wachtwoord, bijvoorbeeld de eerste letters van de titel van een liedje of het laatst gelezen boek. Wissel de letters af met hoofdletters, cijfers en tekens. Gebruik geen namen, woorden of opeenvolgende letters of cijfers. Geen wachtwoord mag hetzelfde zijn. Moet je te veel wachtwoorden onthouden? Gebruik dan een met een complex wachtwoord beveiligd bestand, bijvoorbeeld in excel.

Werk je thuis of elders dan heb je toestemming van je manager nodig. Gebruik je virtuele werkplek en PGGM internet applicaties alleen via https://werkplek.pggm.nl. Werk je elders, overtuig jezelf dan dat je op een veilige pc werkt, voorzien van actuele beveiligingsupdates en antivirussoftware. Zodra je je werkplek verlaat op het werk, thuis of elders vergrendel dan je pc met Ctrl Alt Del enter of Windows-L of sluit je pc af met Ctrl+Alt+F12 of druk op de groene knop.

Mobiel

Je bent persoonlijk verantwoordelijk voor de aan jou ter beschikking gestelde apparatuur en software. Laat draagbare apparatuur niet onbeheerd achter.
Zakelijk gebruik van je mobile device mag alleen met de GOOD app, zie QRC.
Voor een zelf meegebrachte laptop gebruik je het wifi netwerk (wifi-mobile, ww=mobile01). Een laptop mag niet aan een netwerkkabel gekoppeld worden.

Veilig omgaan met informatie

Binnen PGGM hebben we informatie ingedeeld in vier categorieën: geheim, vertrouwelijk, niet vertrouwelijk en openbaar. In de richtlijn classificatie worden deze categorieën toegelicht. Voor elke categorie gelden eisen voor het gebruik en de beveiliging. Zorg dat je deze eisen toepast.

- Als je niet zeker weet of informatie vertrouwelijk is, vraag je manager of behandel het als vertrouwelijk. Een vuistregel is dat informatie vertrouwelijk is wanneer het privacygevoelig is, wanneer je vermoed dat openbaarmaking imagoschade kan veroorzaken of door hackers misbruikt kan worden (bijvoorbeeld welke software we gebruiken of metagegevens in een te publiceren document).
- Stel je zelf vertrouwelijke informatie samen, bewaar dit dan op een veilige netwerkmap of sharepoint werkruimte. Hiervan worden dagelijks back-ups gemaakt. Controleer zelf (of via je manager) dat de toegang tot de informatie inderdaad beperkt is.
- Voor toegang tot applicaties en vertrouwelijke informatie heb je autorisaties nodig. Deze autorisaties zijn strikt persoonlijk. Deel vertrouwelijke informatie niet met anderen. Sluit applicaties af als je ze niet gebruikt.
- Ruim informatie op papier of whiteboard, in je kast of thuis, veilig op.
- Uitwisselen van vertrouwelijke of geheime informatie met partijen buiten PGGM doe je via:
    - Zet #Securemail# voor het onderwerp. Zie QRC Secure Email;
    - Een met bitlocker beveiligde usb-stick;
    - Een sharepoint teamwerkruimte voor als je grote bestanden moet uitwisselen.
- Gebruik voor bedrijfsinformatie geen privé mail of online opslag diensten zoals Dropbox, Skydrive, Evernote, Slideshare, Google Drive, Wetransfer, Google-docs, Icloud, of Onenote.

Email en internet

Het privé gebruik van email en internet is toegestaan mits rekening gehouden wordt met het belang van onze klanten en PGGM. Doe privézaken zoveel mogelijk via het Wifi netwerk om de risico's op malware en hackers zo klein mogelijk te houden. Het gebruik en het monitoren van internet en emailis is aan strenge regels onderworpen die voor iedereen gelden en zijn te vinden in het Protocol privacy e-mail en internetgebruik bij PGGM.

Open geen bijlagen en klik niet op linkjes in onverwachte e-mailberichten . Doe je dit per ongeluk toch, of heb je waarschuwingen genegeerd, let dan extra goed op of er ongebruikelijke dingen gebeuren. Vertrouw je het niet, zet je pc niet uit maar bel direct het IFS Service Point (9777). Tijdige melding kan heel veel ellende voorkomen.

Gebruik van sociale media (Linkedin, Facebook, Twitter, etc.)

Als je te linken bent met PGGM, vertegenwoordig je ook PGGM. Wees professioneel, vriendelijk, discreet en authentiek. Zie ook social media richtlijnen.

Meld informatiebeveiligingsincidenten

Dit zijn situaties waarin de maatregelen op het gebied van informatiebeveiliging niet gewerkt hebben. Er is bijvoorbeeld informatie bij onbevoegden terecht gekomen, informatiesystemen zijn niet beschikbaar of bevatten fouten. Of er gebeuren ongebruikelijke dingen op je pc. Heb je het vermoeden dat je te maken hebt met een incident, meld dit bij je manager en neem ook contact op met het IFS Servicepoint (toestel 9777) als er directe maatregelen nodig zijn.

Meer informatie over informatiebeveiliging vind je op de teamsite van APC.