De kwaliteitsstandaarden van Quality Contacts - 2022

Kwaliteit zit besloten in onze naam 'Quality Contacts'. Daarom streven wij ernaar om hét contactcenter te zijn dat bekend staat om kwaliteit, kennis van zaken, een uitstekende, betrouwbare en veilige dienstverlening en een hoog serviceniveau, wat leidt tot duurzame relaties tussen onze medewerkers, opdrachtgevers en leveranciers. Dit krijgt onder andere vorm door het feit dat wij alle data en (gevoelige) informatie vertrouwelijk behandelen en de performance van onze systemen en medewerkers garanderen.

Om deze kwaliteit te bereiken en ook vast te houden heb jij, als onze collega en ambassadeur van het bedrijf, een zeer belangrijke rol. Lees hier hoe je ons kan helpen:

Tips delen!
Om beter te worden in wat we doen, zijn jullie onze oren en ogen. Hopelijk wil je dit ook met ons delen, zodat alle collega's er van kunnen profiteren. Je kan denken aan het vereenvoudigen van de kennisbank, het bespreken van een bepaald onderwerp in MijnQC of een tip op het gebied van informatiebeveiliging. Geef al je tips daarom door aan je teamleider/leidinggevende.

Informatiebeveiliging
Onze core business bestaat uit informatie/data/(persoons)gegevens. Daar willen wij zo veilig mogelijk mee om gaan, zodat ze in betrouwbare handen zijn en niet toegankelijk voor anderen. Door onderstaande basiselementen toe te passen in je werk gaan we dit samen een stukje veiliger maken.

Clear screen: vergrendel je scherm bij het verlaten van je werkplek.

Clean desk:
en laat geen gegevens slingeren.

Sterke wachtwoorden: maak altijd gebruik van verschillende leestekens, hoofdletters en kleine letters, maar ook cijfers en veel teken en gebruik niet telkens dezelfde wachtwoorden.

Communiceren: verstuur persoonsgegevens nooit digitaal, niet via WhatsApp, niet via Slack etc. Maak ook geen screenshots of foto's van persoonsgegevens.

Deuren gesloten: de deuren die te openen zijn met een keytag mogen nooit open staan. Zorg ook dat je niet zomaar iemand zonder keytag binnen laat.

Maar ook naast de basisprincipes van informatiebeveiliging zijn er nog een aantal aanvullende acties die jij kunt doen om het nog veiliger te maken (ook voor jou in je privé-omgeving):

- Zorg dat je uitlogt uit alle systemen/programma's aan het einde van je werkdag.
- Maak geen gebruik van de USB poorten in je computer/laptop (deze zijn alleen voor je headset, muis en toetsenbord).
- Gebruik je in bruikleen genomen computer/laptop alleen voor QC.
- Laat je laptop/mobiele telefoon van QC nooit onbeheerd achter.
- Berg (tijdens het werken) je mobiel op in je tas of in een kluisje.
- Maak nooit gebruik van een openbare Wifi netwerk.
- Deel geen gegevens over je collega's zonder hun toestemming.

Informatiebeveiligingsincident
Bij een (informatie)beveiligingsincident is de veiligheid van informatie/data/(persoons)gegevens in het geding. Dit kan wanneer werkprocessen langdurig stil komen te liggen of serieuze schade ontstaat of kan ontstaan, door de volgende drie redenen:

Beschikbaarheid
De veiligheid van informatie is in het geding als deze informatie niet beschikbaar is. Bijvoorbeeld als een systeem (zoals Teleknowledge of het CRM systeem van onze opdrachtgever) is uitgevallen of zeer traag is waardoor je jouw werk niet uit kan voeren.

Integriteit
De integriteit van informatie is een issue wanneer informatie niet overeenkomt met de werkelijkheid. Informatie hoort juist, volledig en actueel te zijn. Dit betekend dat informatie in de systemen moeten kloppen en up to date moeten zijn.

Vertrouwelijkheid
Als het gaat om vertrouwelijkheid dan houdt dit in dat alleen de mensen die er recht op hebben die informatie mogen inzien en er (eventueel) iets mee mogen doen. De vertrouwelijkheid kan al een probleem zijn wanneer een e-mail verstuurd is naar de verkeerde persoon.

Klopt er iets niet aan één van deze drie punten dan is er sprake van een informatie beveiligingsincident. En zoals je zal begrijpen willen wij dit niet, omdat informatie onze core business is binnen Quality Contacts.

Informatiebeveiligingsincident → datalek
Heb je het vermoeden dat informatie bij de verkeerde persoon terecht is gekomen of in te zien is door iemand die hier geen recht op heeft (de vertrouwelijkheid is een probleem), dan kan er sprak zijn van een datalek. Meld alle situaties waarbij informatie mogelijk 'gelekt' is direct. In deze zin zijn drie aspecten belangrijk:

- Dit kan informatie/data/(persoons)gegevens zijn van de klanten van onze opdrachtgevers, maar ook van collega's (staf en agents) of gegevens van opdrachtgevers of leveranciers.
- Daarbij gaat het dus om situaties waarbij mogelijk gelekt is. Maak niet zelf de afweging of het een datalek is en vel ook geen oordeel, dit laat je over aan de afdeling kwaliteit, ICT en de operationeel manager.
- Direct is zonder vertragen, neem dus niet eerst even pauze, NEE meld het meteen!

Melden doe je zo: stuur een e-mail naar **security@qualitycontacts.nl**.

Servicedesk ICT
Heb je problemen op ICT vlak, het inloggen op je computer/laptop lukt bijvoorbeeld niet of je muis is stuk? Neem dan contact op met de ICT servicedesk via 038 - 200 65 41 (op werkdagen bereikbaar van 8.00 tot 21.00 uur en op zaterdag van 10.00 tot 16.00 uur) of ict@qualitycontacts.nl.

Door rekening te houden met alle punten uit dit document, maken wij het samen een stukje digitaal veiliger bij Quality Contacts. **Dank daarvoor!**

Veilige digitale groet,

Quality Contacts

Kim, Pjotr en Frank
Management Team