Gedragscode telewerken GGD GHOR Nederland

Deze gedragscode geeft regels voor externen die thuis werken aan een opdracht van GGD GHOR Nederland en/of de GGD. Deze gedragscode behandelt wat er van je wordt verwacht, en hoe je om dient te gaan met je werkzaamheden als externe medewerker van GGD GHOR Nederland, vanuit een externe locatie.

Inleiding

Telewerken is een verzamelterm voor alle vormen waarin een medewerker van GGD GHOR Nederland, beeldschermwerk verricht vanaf een andere locatie dan de gebouwen van GGD GHOR Nederland. Aan telewerken zijn risico's verbonden, zoals het risico dat informatie in handen komt van een buitenstaander. Om deze risico's in te dammen, is deze gedragscode opgesteld.

Doelstelling

De doelstelling van deze gedragscode is het maken van heldere afspraken over telewerken, om de bijkomende risico's te ondervangen.

Toepassingsbereik

De gedragscode ziet op alle vormen van beeldschermwerken vanaf een andere locatie dan een toegewezen/eigen werkplek binnen de gebouwen van GGD GHOR Nederland, door alle medewerkers, intern, extern, vertegenwoordigers en overige personen die werkzaam zijn voor of namens GGD GHOR Nederland.

1. Inleiding

Om telewerken op een juiste en veilige manier mogelijk te maken, heeft GGD GHOR Nederland een beveiligde omgeving opgezet. Van de medewerker wordt verwacht dat deze ook maatregelen neemt, om de gegevens waarmee wordt gewerkt veilig te houden.

2. Aanwijzingen voor het gebruik

Voor het werken op afstand, geeft GGD GHOR Nederland een aantal aanwijzingen.

- Voor werken op afstand wordt door GGD GHOR Nederland een werkomgeving op afstand beschikbaar gesteld, die benaderd kan worden via apparatuur (PC en laptop voor werkzaamheden en telefoon voor authenticator app en servicedesk functie) van de medewerker.
- De toegang tot de thuiswerkomgeving wordt alleen verleend op basis van multifactor authenticatie. Hiervoor dient de medewerker een authenticator app op de mobiele telefoon van de medewerker te worden geïnstalleerd.
- De medewerker maakt enkel gebruik van de thuiswerkomgeving die door de GGD GHOR Nederland beschikbaar is gesteld. Andere programma's of applicaties mogen niet worden gebruik in het kader van de opdracht of werkzaamheden gelieerd aan de opdracht worden uitgevoerd.
- Indien GGD GHOR Nederland verzoekt om software te installeren om de opdracht uit te voeren of de computer juist te beveiligen, dienen medewerkers dit te doen.
- Illegale software mag niet worden gebruikt voor de uitvoering van de opdracht.
- Het verbod op ongewenst gebruik in de (fysieke) kantooromgeving geldt ook als dat via de eigen computer plaatsvindt.

3. Beveiligingsmaatregelen

3.1. Aan de medewerker wordt voor het telewerken toegang gegeven tot een beveiligde omgeving waarin de medewerker de opdracht kan uitvoeren. De gegevens mogen niet buiten de beveiligde omgeving worden verwerkt. Dit houdt onder andere in dat de medewerker geen andere programma's of applicaties mag gebruiken om de opdracht mee uit te voeren en geen kopieën, screenshots, prints, etc. mag maken. Daarnaast mag de medewerker geen gegevens met betrekking tot de opdracht of gelieerd aan de opdracht opslaan op de privéapparatuur.

3.2. De medewerker zorgt dat de apparatuur waar op wordt bewerkt adequaat wordt beveiligd. Dit betekent dat minstens een virusscanner is geïnstalleerd die up-to-date is, en dat regelmatig beveiligingsscans worden uitgevoerd zodat bedreigingen tijdig worden gevonden en opgelost. Daarnaast zorgt de medewerker dat de updates van de apparatuur zijn geïnstalleerd. Indien de medewerker merkt dat het apparaat is geïnfecteerd met een virus of een systeem of persoon op andere wijze onrechtmatige toegang tot het apparaat kan verkrijgen of heeft gekregen, dient de werknemer per direct het protocol melden datalekken van de organisatie waarvoor hij/zij werkzaam is te volgen. De organisatie draagt vervolgens zorg voor de directe melding hiervan aan GGD GHOR Nederland via de meldprocedure.

3.3. Voorzie de apparatuur tenminste van de volgende aspecten:
- Up-to-date virusscanner;
- Personal Firewall;
- Anti malware-tool;
- Schermvergrendeling met wachtwoord;
- Up-to-date besturingssysteem en applicaties.

3.4. De medewerker zal geen inloggegevens delen met anderen in de omgeving of collega's delen of deze ergens noteren waar deze kunnen worden gevonden.

3.5. De medewerker wisselt geen inloggegevens of gegevens uit met derden, waarvan niet duidelijk is of deze derden de gegevens mogen ontvangen (phishing). Indien de medewerker twijfelt over de identiteit van de derde, neemt de medewerker contact op met de contactpersoon bij GGD GHOR Nederland om te verifiëren of de gegevens mogen worden uitgewisseld.

3.6. Activiteiten van medewerkers worden gelogd. Deze logging wordt regelmatig gecontroleerd. Dit is GGD GHOR Nederland wettelijk verplicht te doen.

4. Werkplek

4.1. De werkplek moet zo ingericht zijn dat anderen niet op het scherm kunnen kijken en gesprekken die gevoerd worden in het kader van de opdracht niet kunnen worden gehoord. De gegevens die in het kader van de opdracht worden verwerkt zijn vertrouwelijk en mogen daarom niet door anderen worden gezien en/of gehoord.

4.2. De werkplek moet zo zijn ingericht dat de medewerker geconcentreerd kan werken.

4.3. Eventuele documenten met betrekking tot de opdracht en/of apparatuur waarop de thuiswerkomgeving open staat, mogen niet onbeheerd worden achtergelaten. Indien de medewerker tijdelijk de werkplek verlaat, moet de laptop worden vergrendeld of de thuiswerkomgeving worden vergrendeld/afgesloten, zodat deze niet onrechtmatig kan worden ingezien.

4.4. De werkplek moet zijn voorzien van een beveiligde netwerkverbinding, met tenminste een wpa 2 beveiligingsniveau en een sterk wachtwoord. Het beveiligde netwerk moet daarbij een beperkt aantal gebruikers hebben, zoals leden van het gezin en mag niet worden gebruikt door een grote groep gebruikers, zoals een appartementencomplex met gedeeld internet. Voor het netwerk met een sterk wachtwoord zijn ingesteld, dat bestaat uit:

- Minimaal 8 karakters;
- Minimaal 1 hoofdletter;
- Minimaal 1 cijfer;
- Minimaal 1 speciaal teken;
- Gebruik geen voor de hand liggende woorden of reeksen (zoals Qwerty, Welkom01);
- Gebruik geen persoonlijke gegevens (zoals geboortedata, namen van kinderen).

4.5. Openbare netwerken mogen niet worden gebruikt. Ook netwerken waarvan het wachtwoord bekend is, zoals in een restaurant waar mensen het wachtwoord kunnen opvragen, mogen niet worden gebruikt. Via dit soort onbeveiligde verbindingen kan het netwerkverkeer namelijk worden gemonitord.

4.6. De medewerker mag geen gebruik maken van publiek beschikbare apparaten of apparaten die niet van de medewerker zelf zijn.

4.7. Laat de mobiele devices niet in een onbeheerd vervoermiddel liggen en vervoer deze niet in het zicht. Bijvoorbeeld op de voorstoel, achterbank of op de vloer.

4.8. Aanwijzingen van GGD GHOR Nederland die betrekking hebben op het verzenden en ontvangen van gevoelige informatie, moeten worden opgevolgd.

4.9. Aanwijzingen van GGD GHOR Nederland die betrekking hebben op het omgaan met wachtwoorden en login-procedures, moeten worden opgevolgd.

5. Uitlekken van gegevens en verlies van apparatuur en/of gegevens

Indien gegevens uitlekken of kunnen uitlekken, gegevens verloren gaan of mogelijk zijn gegaan, of apparatuur waarop de thuiswerkomgeving wordt gebruikt wordt verloren of gestolen, moet hiervan direct een melding worden gedaan conform het protocol melden datalek binnen de organisatie. De organisatie moet uiterlijk binnnen 4 uur hiervan een melding kunnen maken bij GGG GHOR Nederland volgens de datalekprocedure.

6. Gevolgen van niet-naleving van de gedragscode

Indien de medewerker de regels gesteld in deze gedragscode niet naleeft, kan dit gevolgen hebben voor de verdere uitvoering van de opdracht en kan de geleden schade worden verhaald op de medewerker.