NEN 7510 thema	**Wie**
Beheer van bedrijfsmiddelen	GGD + landelijke partners
Naleving	GGD + landelijke partners
Toegangs-beveiliging	GGD + landelijke partners
Veilig personeel	GGD + landelijke partners
Veilig personeel	GGD + landelijke partners

Toegangsbeveiliging	GGD + landelijke partners
Incident management	GGD + landelijke partners

Actie
Hanteer eisen, pas maatregelen toe en richt toezicht in voor de beveiliging van de **BCO werkplekken** conform NEN 7510. Stel gebruikers op de hoogte hoe ze veilig kunnen werken.
Richt **auditlogging** in voor de active directory (**AD**) of directory service**, conform 7513.** Log in ieder geval: - alle gebeurtenissen die de toegangsregeling betreffen. Het gaat daarbij in elk geval om gebeurtenissen die betrekking hebben op de structuur van de instelling, de toegangsregeling en het instellen van toestemmingsprofielen. - bevoegdheden: creëren, wijzigen en of verwijderen van bevoegdheden die gelden voor toegang tot applicatiefuncties en gegevensgroepen;
Controleer periodiek of **alle toekomstige en huidige gebruikers** voor het portaal een **uniek AD gebruikersaccount** hebben
Controleer periodiek of **alle toekomstige en huidige gebruikers** voor het portaal een **VOG** hebben
Controleer of **alle toekomstige en huidige gebruikers** voor het portaal een **geheimhoudingsverklaring** hebben getekend

Houd het **Join-Move-Leave proces** bij: Elke wijziging aan rollen vertrekkende medewerkers (leave), medewerkers met een andere rol (move) en nieuwe medewerkers (join) moet direct worden verwerkt in de AD.

De organisatie en beheerder van een AD is zelf verantwoordelijk voor het bijhouden van een actueel AD en het juist toekennen van de gebruikersrollen. Het niet juist bijhouden van de AD kan leiden tot onbevoegde toegang tot het dossier van een index.

Controleer periodiek of **alle huidige gebruikers de juiste rollen** hebben toebedeeld gekregen.

Registreer incidenten op het gebied van onrechtmatig gebruik van de corona gerelateerde applicaties.

Informeer de met governance belaste organen (zoals FG) binnen de GGD en GGD GHOR (SOC).

Praktische aanwijzingen

1. Gebruik geen BYOD maar door de organisatie beheerde systemen. Zorg dat alle USB poorten zijn gesloten.
2. Stel screenlock in voor inactiviteit na 5 mins
3. Lock het scherm wanneer de werkplek verlaten wordt (Windows-L).
4. Voer een clean desk policy in, geen privacy gevoelige informatie op bureau, whiteboards etc
5. Zorg voor up-to-date anti-4-us en anti-malware software, en voor een up-to-date browser.
6. Voorzie elke werkplek van do's en dont's op het gebied van informatie beveiliging

1. Richt dit in samen met IT en Security.
2. Alle logs dienen voor de duur van de Corona crisis bewaard te worden. Later zal de uiteindelijke bewaartermijn worden gecommuniceerd.
3. Logs mogen niet gewijzigd worden of ingezien door onbevoegden.
4. Logs kunnen worden gebruikt voor forensisch onderzoek, en dienen beschikbaar te kunnen worden gemaakt.

1. Nieuwe medewerkers (joiners) kunnen pas worden opgevoerd nádat ze een Contract, VOG en geheimhoudingsverklaring hebben getekend.
2. Elke week dienen de AD gebruikers accounts te worden vergeleken met de medewerkers in dienst. De verschillen moeten verklaard zijn. De uitkomst van deze verklaring dient te zijn vastgelegd.
3. Niet persoonsgebonden accounts dienen een eigenaar te hebben, en er dient een verklaring te zijn voor gebruik en noodzaak.

1. VOG's dienen opnieuw te worden aangevraagd na de verjaartermijn.
2. Houd register bij met goedgekeurde VOG's, en vergelijk deze jaarlijks met het personeelsbestand.
3. Leg uitkomst van deze controle vast.

(nog uitzoeken wie termijn bepaalt)

1. Geheimhoudingsverklaringen dienen opnieuw te worden aangevraagd na de verjaartermijn.
2. Houd register bij met goedgekeurde Geheimhoudingsverklaringen, en vergelijk deze jaarlijks met het personeelsbestand.
3. Leg uitkomst van deze controle vast.

(nog uitzoeken wie termijn bepaalt)

1. Leg iedere wijziging vast in een ticket.

2. Aanvragen voor J-M-L moeten geautoriseerd worden, en deze autorisatie moet zijn vastgelegd.

3. Autorisaties op basis van vooraf gedefinieerde profielen.

4. Elke week dienen de AD gebruikers én hun rol te worden vergeleken met de medewerkers in dienst en hun rol in het Personeelssysteem. De verschillen moeten verklaard zijn. De uitkomst van deze verklaring dient te zijn vastgelegd.

---

1. Maak van ieder incident een ticket.

2. Leg alle documentatie en besluitvorming vast in een dossier.

GGD Zaanstreek-Waterland

Geregeld

Screenlock is GGD-organisatiebreed ingesteld op 15 minuten

Algemene werkinstructie / beleid, wat bekend is bij BCO-medewerkers. Aanscherping is mogelijk op het vlak van awareness en controle

Algemene werkinstructie / beleid, wat bekend is bij BCO-medewerkers. Aanscherping is mogelijk op het vlak van awareness en controle

Geregeld

Niet aanwezig

Er is geen auditloggin voor de AD operationeel. Technisch gezien is dit geen enkel probleem om dit te activeren, echter het ontbreekt momenteel aan beleid hieromtrent. Via de werkgroep Dataveiligheid wordt dit ontwikkeld.

Zie boven

Zie boven

Zie boven

Voor GGD-medewerkers is dit via PenO gewaarborgd. Echter, BCO medewerkers zijn in de regel ingehuurd via uitzendbureaus. Genoemende voorwaarden zijn inderdaad vastgelegd in het contract met de uitzendorganisatie. GGD controleert zelf de VOG en geheimhoudingsverklaring bij aanvang van de inzet van de uitzendkracht. Naleving in de praktijk verdient nadere aandacht.

Hierop is momenteel geen beleid.

We hebben geen niet-persoongebonden accounts in de AD t.a.v. BCO Portaal. Binnen de gehele AD gaat het om 3-4 accounts, die alleen gebruikt kunnen worden om toegang te krijgen tot een device, om vervolgens toegang te krijgen tot een SaaS-applicatie. Voor dat laatste is dan weer wel een persoongebonden account nodig.

Geen beleid over. Verjaartermijn is een misleidende termijn. Een VOG is een verklaring waaruit blijkt dat het (justitiële) verleden geen bezwaar vormt voor het vervullen van een specifieke taak of functie binnen de GGD. Bij de beoordeling van een VOG-aanvraag kijkt Justis of er strafbare feiten op naam van de medewerker staan die een risico vormen voor de functie of het doel waarvoor de VOG aanvraagt. Het is een momentopname.

Bij houden van het register is (contractueel vastgelegd) de verantwoordelijkheid voor uitzendorganisaties. VOG van GGD-medewerkers zitten in het personeelsdossier

Hierop is momenteel geen beleid.

Er is geen verjaartermijn gedefinieerd. Een geheimhoudingsverklaring geldt gedurende het dienstverband en zelfs daarna. Deze eis verdient nadere toelichting

Bij houden van het register is (contractueel vastgelegd) de verantwoordelijkheid voor uitzendorganisaties. Geheimhoudingsverklaringen van GGD-medewerkers zitten in het personeelsdossier. Periodieke controle vindt niet plaats

Controle vindt niet plaats

Voor Join en Leave is dit voor HPZone Light geregeld via het ticketingsysteem Facilitor. Bij introductie BCO Portaal wordt dat ook ingezet voor Move. Autorisaties voor gebruikers worden verleend door de Coördinator Corona, X op dit moment. Voor BCO Portaal zal dit m.b.t. werkverdeler en gebruiker ingeregeld worden. Organisatorisch is dit voorbereid. Op ad hoc basis vindt controle plaats, meestal bij proceswijzigingen en/of incidenten. Vastlegging daarvan vindt niet plaats
Gewaarborgd in de procedure Datalek M.b.t. intern GGD en de Autoriteit Persoonpersoonsgegevens is dat een onderdeel van procedure Datalek. SOC GGD GHOR wordt hierin niet meegenomen.