| NEN 7510 thema | Wie | Actie | Praktische aanwijzingen | 20218 |
|---|---|---|---|---|
| Beheer van bedrijfsmiddelen | GGD + | Hanteer eisen, pas maatregelen toe en richt toezicht in voor de beveiliging van de **BCO werkplekken** conform NEN 7510. | 1. Gebruik geen BYOD maar door de organisatie beheerde systemen. Zorg dat alle USB poorten zijn gesloten. | Geborgd by design. Er zijn enkele uitzonderingen, maar dit gebeurt weinig en staat gelogd. |
| | landelijke partners | Stel gebruikers op de hoogte hoe ze veilig kunnen werken. | 2. Stel screenlock in voor inactiviteit na 5 mins | Interne discussie geweest, uitkomst is 15 minuten |
| | | | 3. Lock het scherm wanneer de werkplek verlaten wordt (Windows-L). | Regulier bewustwordingsproces |
| | | | 4. Voer een clean desk policy in, geen privacy gevoelige informatie op bureau, whiteboards etc | Clean desk beleid stedelijk aanwezig. Regulier bewustwordingsproces. |
| | | | 5. Zorg voor up-to-date anti-4-us en anti-malware software, en voor een up-to-date browser. | Geborgd via regulier beheer. |
| | | | 6. Voorzie elke werkplek van do's en dont's op het gebied van informatie beveiliging | |
| Naleving | GGD + | Richt **auditlogging** in voor de active directory (**AD**) of directory service**, conform 7513**. Log in ieder geval: | 1. Richt dit in samen met IT en Security. | In- en uitloggen wordt gelogd, gegevens beschikbaar in SIEM oplossing. |
| | landelijke partners | - 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. | 2. Alle logs dienen voor de duur van de Corona crisis bewaard te worden. Later zal de uiteindelijke bewaartermijn worden gecommuniceerd. | Wordt standaard 6 maanden bewaard |
| | | - bevoegdheden: creëren, wijzigen en of verwijderen van bevoegdheden die gelden voor toegang tot applicatiefuncties en gegevensgroepen; | 3. Logs mogen niet gewijzigd worden of ingezien door onbevoegden. | Alleen systeembeheerders hebben toegang. Meesten hebben enkel leesrechten, slecht 2-3 personen hebben schrijfrechten |
| | | | 4. Logs kunnen worden gebruikt voor forensisch onderzoek, en dienen beschikbaar te kunnen worden gemaakt. | Is mogelijk |
| Toegangs-beveiliging | GGD + | Controleer periodiek of **alle toekomstige en huidige gebruikers** voor het portaal een **uniek AD gebruikersaccount** hebben | 1. Nieuwe medewerkers (joiners) kunnen pas worden opgevoerd nádat ze een Contract. VOG en geheimhoudinesverklaring hebben getekend. | Account wordt vrijgegeven nadat aan genoemde voorwaarde is voldaan |
| | landelijke partners | | 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 | Wordt maandelijks uitgevoerd |
| | | | 3. Niet persoonsgebonden accounts dienen een eigenaar te hebben, en er dient een verklaring te zijn voor gebruik en noodzaak. | Bij aanvraag dient eigenaar, noodzaak en gebruik te worden aangegeven |
| Veilig personeel | GGD + | Controleer periodiek of **alle toekomstige en huidige gebruikers** voor het portaal een **VOG** hebben | 1. VOG's dienen opnieuw te worden aangevraagd na de verjaartermijn. | Geldig VOG is nodig voor aanstelling. Verjaringstermijn is nog niet van toepassing voor medewerkers team Coronal. |
| | landelijke partners | | 2. Houd register bij met goedgekeurde VOG's, en vergelijk deze jaarlijks met het personeelsbestand. | Wordt uitgevoerd in samenspraak met automatisering. Indien na controle blijkt dat er toch geen sprake is van goedgekeurd VOG wordt acoount accuur geblokkeerd. |
| | | | 3. Leg uitkomst van deze controle vast. (nog uitzoeken wie termijn bepaalt) | Uitkomst wordt door projectleider personeel vastgelegd |
| Veilig personeel | GGD + | Controleer of **alle toekomstige en huidige gebruikers** voor het portaal een **geheimhoudingsverklaring** hebben getekend | 1. Geheimhoudingsverklaringen dienen opnieuw te worden aangevraagd na de veriaartermiin. | Zie antwoord hiervoor |
| | landelijke partners | | 2. Houd register bij met goedgekeurde Geheimhoudingsverklaringen, en vereelijk deze iaarliiks met het personeelsbestand. | Loopt parallel met VOG procedure |
| | | | 3. Leg uitkomst van deze controle vast. (nog uitzoeken wie termijn bepaalt) | |
| Toegangsbeveiliging | GGD + | 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. | 1. Leg iedere wijziging vast in een ticket. | Uitgegezet bij de betreffende afdeling, antwoord volgt. Update: Elke join wordt vastgelegd in een ticket en verwerklt in AD. Leave en move wordt via gedelegeerden vanuit de teamleiders via de mail doorgegeven aan de functioneel beheerders en verwerken dit vervolgens in de betreffende systemen en AD. Daarnaast vindt periodiek een controle plaats en worden 'missers' gecorrigeerd |
| | landelijke partners | 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 | 2. Aanvragen voor J-M-L moeten geautoriseerd worden, en deze autorisatie moet zijn vastgelegd. | Uitgegezet bij de betreffende afdeling, antwoord volgt. |
| | | Controleer periodiek of **alle huidige gebruikers de juiste rollen** hebben toebedeeld gekreeen. | 3. Autorisaties op basis van vooraf gedefinieerde profielen. | Uitgegezet bij de betreffende afdeling, antwoord volgt. Update: Zie hiervoor bij toegangsbeveiliging punt 1 |
| | | | 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. | Uitgegezet bij de betreffende afdeling, antwoord volgt. |
| Incident management | GGD + | Registreer incidenten op het gebied van onrechtmatig gebruik van de corona gerelateerde applicaties. | 1. Maak van ieder incident een ticket. | Conform incidentmanagement proces. |
| | landelijke partners | Informeer de met governance belaste organen (zoals FG) binnen de GGD en GGD GHOR (SOC). | 2. Leg alle documentatie en besluitvorming vast in een dossier. | Uitgegezet bij de betreffende afdeling, antwoord volgt. |