1. Fysieke beveiliging ruimtes en informatie	*Worden ruimtes met (digitale) cliënt- of medewerkersgegevens beveiligd?*	
2. Gebruikersaccounts	*Heeft ieder medewerker zijn eigen account/gebruikersnaam op de werkplek (computer) en voor de verschillende applicaties?*	
3. Toegang tot applicaties en informatie	*Zijn mappen/bestanden afgeschermd zodat niet alle medewerkers bij alle mappen kunnen (b.v. niet bij personeelsgegevens, of alleen bij eigen clienten)*	
	Zijn uw applicaties/ systemen voorzien van 2FA (two factor authentification)?	*Als u inlogt bij ONS dient u met de app van ONS gebruik te maken van een tweestapsverificatie. Er moet namelijk aangetoond worden dat de verzender daadwerkelijk de persoon is voor wie hij zich uitgeeft. Dit is ook nodig voor uw office producten (Outlook, Zorgmail).*
	Zijn er binnen uw applicaties /systeem autorisaties en rechten op verschillende niveaus ingesteld?	*Zoals toegang tot een bepaalde mailbox of toegang tot bepaalde schijven.*
4. Wachtwoorden	*Weet alleen de medewerker zijn/haar eigen wachtwoord?*	*Het is niet de bedoeling dat deze gegevens gedeeld worden met collega's of dat een beheerder er toegang toe heeft.*
5. Wachtwoordeisen	*Worden de volgende eisen gesteld aan wachtwoorden nageleeft?*	*n.v.t.*
	Minimaal 7 karakters:	
	Gebruik van speciale tekens:	*zoals ?#!&*

6. Beveiligen van opslag	*Hebt u in uw beleid opgenomen en actief in gesprekken met uw medewerkers dat het verboden is b.v. gegevens van clienten en medewerkers op een onbeveiligde laptop of usb-stick mee naar huis te nemen? Zie toelichting over wat een goede beveiliging is.*	*Versleuteling of encryptie is een beveiligingsmethode waarbij informatie of informatiedragers beveiligd worden met een wachtwoord. Zonder dit wachtwoord is de informatie niet leesbaar. Voor computers en laptops wordt Bitlocker vaak gebruikt.*
7. Veilig e-mailen	*Als er client- of medewerkergegevens worden gemaild wordt dat dan altijd gedaan via Zorgmail?*	*Zorgmail voldoet volgens de AVG richtlijnen aan het veilig verzenden van persoonsgegevens. Bij het delen van gegevens let iedereen alijd op dat niet zomaar voor- en achternaam en / of BSN wordt gedeeld.*
	Als client- of medewerkergegevens worden gemaild buiten de organisatie (naar een niet zorgmail account) wordt altijd zorgmail gebruikt met de veiilig verzenden knop?	*Controleer of de veilig verzenden knop bij iedere medewerker beschikbaar staat.*
	Als client- of medewerkergegevens worden gemaild wordt altijd zorgmail gebruikt?	*Zorgmail voldoet volgens de AVG richtlijnen aan het veilig verzenden van persoonsgegevens.*
8. Back-ups	*Maakt u backups van client- en medewerkersgegevens?*	*Het is de bedoeling dat u alleen gebruik maakt van clilentgevens via het clientadministratie systeem ONS en via Zorgmail voor delen van gegevens. Voor uw personeel hanteert u een beveiligd personeelsdossier / applicatie. Mocht u gebruik maken van backups zie locatie eisen in het volgende onderdeel.*
9. Back-up locatie	*Staat de back-up op een veilige, afgesloten locatie?*	*Het is belangrijk dat de back-up schijf niet op de zelfde locatie staat als de computerruimte.*
10. Locken van de computer	*Wordt de computer vergrendeld als iemand van zijn werkplek weg gaat en gebeurt dit automatisch na ongeveer 5 minuten?*	*Instellen op alle hardware die u en de medewerkwer gebruikt.*

11. Clean desk policy	*Worden er geen papieren op de bureaus achter gelaten (met clientgegevens) of wordt de deur dan altijd op slot gedaan als de werkplek wordt verlaten?*	*Beheer medewerker- en clientgegevens het liefst alleen digitaal, hiervoor hebben we de diverse applicaties. Gegevens dienen altijd versnippert in de prullenbak terecht te komen.*
12. Microsoft versie	*Maakt u gebruik van Microsoft en is dit een versie na 2019 of betreft het Office 365?*	*Een verouderde versie heeft gevolgen voor het veilig delen / beheren van gegevens. Per 31 oktober 2020 beëindigt Microsoft de ondersteuning van Outlook 2010, Zorgmail sluit hierbij aan. Mailen met een verouderde versie is dan niet meer veilig.*
13. Hardware	*Harde schijven encrypted?*	*Dit is voor als er een diefstal is of een laptop kwijt raakt. Dan is de data nooit toegangkelijk.*
14. Netwerk	*Is het netwerk zo ingericht dat gasten/kantoor/personeel netwerken zijn gescheiden?*	*Hiermee wordt bedoeld of er subnets/vlan zijn. Dit om te voorkomen dat er vanuit het netwerk bij gevoelige data kan worden gekomen door onbevoegde mensen.*
	Is uw netwerk juist geconfigureerd (sterke beveiliging)?	*Als het netwerk verkeerd geconfigureerd is kunnen ze een bron van problemen vormen: derden kunnen uw netwerk misbruiken. Sterke beveiliging: WPA.*
	Beschikt uw computer over een firewall en hebt u betaalde virusscanners?	*Als het netwerk onvoldoende beveiligd is kunnen ze een bron van problemen vormen: derden kunnen uw netwerk misbruiken.*