Checklist thuiswerken

Operationeel

Beveiliging digitale werkomgeving		
Actie	**Voorbeelden**	**Uitgevoerd?**
Stel vast of alle werkstations van medewerkers de beschikking hebben over een up-to-date antimalware programma.		
Stel vast dat alle werkstations van medewerkers versleuteld zijn.	Denk hierbij aan BitLocker (Windows) en FileVault (Apple)	
Stel vast dat een werkende VPN verbinding naar de online werkomgeving beschikbaar is en instructies aanwezig zijn voor medewerkers voor het gebruik van de VPN.		
Gebruik MultiFactor authenticatie, voor het op afstand toegang verkrijgen tot een online werkomgeving.	Multi-Factor Authenticatie (MFA) is een authenticatie methode waarbij de gebruiker twee stappen succesvol moet doorlopen om ergens toegang tot te verkrijgen. Denk hierbij aan wachtwoord én een sms token.	
Stel vast dat up-to-date antivirus en firewall zijn geïnstalleerd voor de digitale werkomgeving.		
Stel vast dat het aantal uitgegeven tokens afdoende is om gebruikers veilig te laten inloggen.	Wellicht dat Office 365 met Cloud gebaseerde Outlook, Teams of Sharepoint een goede oplossing is.	
Stel vast dat de applicatie voor remote werk geschikt voor een hoger aantal gebruikers dan normaal.	Hierbij kun je denken aan licenties, capaciteit, en performance van bijvoorbeeld je Citrix ADC of Fortigate VPN omgevingen.	
Stel vast of medewerkers bij het thuiswerken gebruik maken van een controlesysteem waarmee u inzicht heeft op de werkzaamheden van de medewerkers.	Het Europees Verband van Toezichthouders heeft aangegeven dat deze software in nagenoeg alle gevallen niet is toegestaan. Het uitvoeren van een DPIA is noodzakelijk voor het mogen gebruiken van de betreffende software, net als een OR wanneer van toepassing.	
Stel vast dat de autorisatiematrix is gecontroleerd op de toereikendheid van de autorisaties met betrekking tot het remote werken van de organisatie.		
Stel vast dat er een communicatieplan is opgesteld om de communicatie tijdens thuiswerken te kunnen stroomlijnen.		
Stel vast dat back-ups zijn ingericht voor de online werkomgeving.		
Awareness		
Actie	**Voorbeelden**	**Uitgevoerd?**
Stel medewerkers op de hoogte op welke wijze zij phishing mails kunnen herkennen en melden.		
Stel medewerkers op de hoogte dat updates van bedrijfsmiddelen zo snel mogelijk geïnstalleerd dienen te worden.		
Stel medewerkers op de hoogte hoe zij informatiebeveiligingsincidenten en datalekken kunnen herkennen en melden.		
Stel medewerkers op de hoogte hoe zij hun fysieke thuiswerkomgeving in kunnen richten om zo veilig mogelijk te kunnen werken.	Denk hierbij aan het meekijken van familieleden en het werken met het scherm richting een raam.	
Stel medewerkers op de hoogte dat bluetooth verbindingen niet aan staan wanneer dit niet vereist is.	Bluetooth optie muis en toetsenbord.	
Stel medewerkers op de hoogte dat bij elke afwezigheid van het device waar op gewerkt wordt, deze gelockt dient te worden.	Windows toest + L (sneltoets lock)	

Stel medewerkers op de hoogte dat een sterk WiFi-wachtwoord de veiligheid van het netwerk verhoogt.		
Stel medewerkers op de hoogte dat zij een kabel gebruiken om netwerkverbinding te configureren of via een draadloos netwerk met versleuteling.		
Stel medewerkers op de hoogte van het 'Clear Desk' of 'Clear Screen' beleid en dat dit ook bij thuiswerken van toepassing is.		

Tactisch

Change Management

Actie	Voorbeelden	Uitgevoerd?
Stel vast dat het managen van spoedchanges in een remote-werkende organisatie beschreven en gecommuniceerd is naar relevant personeel.		
Stel vast dat redundantie is ingericht om de afgesproken SLA tijden te kunnen bereiken.		

Incident Management

Actie	Voorbeelden	Uitgevoerd?
Stel vast dat voldoende maatregelen zijn ingericht om de bereikbaarheid van de servicedesk te kunnen garanderen.		
Stel vast dat redundantie is ingericht om de afgesproken SLA tijden te kunnen bereiken.		
Stel vast dat er een persoon is aangewezen wanneer er problemen zijn rondom VPN.		
Stel vast dat redundantie van kritische IT-componenten is gewaarborgd.		

Beoordelingen

Actie	Voorbeelden	Uitgevoerd?
Stel vast dat de VPN betrouwbaar is door middel van het uitvoeren van een penetratie test.		
Stel vast dat procedures aanwezig zijn om contacten te behouden met overheidsinstanties en belangengroepen met betrekking tot relevante ontwikkelingen.	Denk hierbij aan het RIVM en het NCSC.	
Installeer een online communicatie- en samenwerkingsplatform.	Bij ontbreken hiervan denk dan aan bijvoorbeeld Google Drive, Dropbox of Office365.	
Stel vast of er Single Points of Knowledge medewerkers zijn en er is ingeregeld hoe deze kennis bij uitval van de medewerker vervangen of opgevangen wordt.	Denk hierbij aan specifieke kennis of specifieke autorisaties.	

Strategisch

Bedrijfscontinuïteit

Actie	Voorbeelden	Uitgevoerd?
Stel vast dat taken en verantwoordelijkheden ten aanzien van het waarborgen van de bedrijfscontinuïteit zijn toegewezen aan de juiste personen.		
Richt een periodieke continuïteitsmeeting in, waarin de huidige ontwikkelingen en benodigde maatregelen worden besproken.		
Opstellen en delen van een beleid voor thuiswerken.		