gemeente Oisterwijk

GEMEENTEBLAD

Officiële uitgave van de gemeente Oisterwijk

Nr. 192461

10 september 2018

Telewerkbeleid gemeente Oisterwijk 2018

1. Doelstelling
De gemeente Oisterwijk hoort beleid, operationele plannen en procedures voor telewerken te ontwikkelen en implementeren.

2. Implementatie

a) Er is een telewerkverklaring met gedragsregels en een geschikte implementatie van de techniek opgesteld t.a.v. telewerken.
b) Er is beleid vastgesteld, met daarin de uitwerking welke systemen vanuit de thuiswerkplek of andere telewerkvoorzieningen mogen worden geraadpleegd. Dit beleid wordt bij voorkeur ondersteund door een MDM-oplossing (Mobile Device Management).
De telewerkvoorzieningen zijn waar mogelijk zo ingericht dat op de werkplek (thuis of op een andere locatie) geen bedrijfsinformatie wordt opgeslagen ('zero footprint') en mogelijke malware vanaf de werkplek niet in het vertrouwde deel terecht kan komen

3. Beleidsuitgangspunten

De gemeente Oisterwijk hanteert de volgende beleidsuitgangspunten en deze zijn ontleend aan de BIG 1.0:
Het opstellen van een bruikleenovereenkomst.
In deze overeenkomst staan afspraken die betrekking hebben op het telewerken.

Afspraken tussen verantwoordelijke en telewerker.
• Afspraken over voortgang, terugkoppeling, bereikbaarheid et cetera.
• Welke apparatuur door de gemeente Oisterwijk is verstrekt en onder welke condities dit is gebeurd.

4. Aanvullende benodigde (technische) voorzieningen en ondersteuning.

In verband met de beveiliging van de informatie moeten onderstaande aanwijzingen door de telewerker worden opgevolgd:
• zorg voor virusprotectie;
• plaats geen gevoelige informatie op mobiele devices of draagbare opslagmedia zonder versleuteling;
• het geheugen van mobiele devices wordt bij voorkeur volledig versleuteld;
• draagbare opslagmedia moet goed worden geëtiketteerd en de gevoeligheid (classificatie) van de inhoud daarvan moet duidelijk worden gemarkeerd. de opgeslagen informatie wordt gewist voordat het device wordt ingeleverd, afgedankt of verkocht;
• 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;
• bescherm mobiele devices, indien mogelijk, tegen diefstal door gebruik te maken van een kabelslot/antidiefstalkabel. Met deze kabel kan het mobiele device gekoppeld worden aan een vast object;
• aanwijzingen die betrekking hebben op het verzenden en ontvangen van gevoelige informatie;
• aanwijzingen die betrekking hebben op het omgaan met wachtwoorden en login-procedures;
• installeer geen ongeautoriseerde hard- en software.
• installeer geen eigen software of download deze niet van een onbekende bron of van het Internet.

Het opstellen van regels voor acceptabel gebruik. Deze regels zijn opgenomen in de Telewerk verklaring.
Binnen de regels voor acceptabel gebruik is aandacht voor:
• Het proces in geval van verlies of diefstal van alle mobiele devices, waarbij meldingen binnen 4 uur gedaan moeten worden.
• Een verbod op het downloaden van illegale software en software uit niet-vertrouwde bronnen.
• Zich houden aan ICT-standaarden en nadere afspraken.
• Het verbod op ongewenst gebruik in de (fysieke) kantooromgeving, geldt ook als dat via de eigen computer plaatsvindt.

Gebruikers hebben kennis van de regels:
• De risico's met betrekking tot telewerken dienen aandacht te krijgen in bewustwordings- en trainingsmateriaal van de gemeente Oisterwijk.
• Illegale software mag niet worden gebruikt voor de uitvoering van het werk.

Toevoegen van regels voor het meenemen van informatie:
• De gemeente Oisterwijk dient ook aandacht te hebben voor de impliciete toestemming aan gebruikers welke informatie zij wel of niet mogen inzien tijdens het telewerken.
• Er dient duidelijk te worden gemaakt dat de medewerker achteraf ter verantwoording geroepen kan worden.

Detailregels om te zorgen voor bescherming van gegevens tijdens het telewerken:
• De gemeente hanteert classificatieregels van gegevens en zorgt voor passende maatregelen om dit bij telewerken (al of niet) te ondersteunen.
• Bedrijfsapplicaties worden bij voorkeur zo aangeboden dat er geen informatie wordt opgeslagen op het device („zero footprint"). Informatie en bedrijfsinformatie van derde partijen, waarvan de gemeente niet de bronhouder is, maar via het platform wordt ontsloten dient te worden versleuteld bij transport en opslag, conform classificatie eisen.
Door het centrale beheer is het mogelijk om met relatief lage beheerinspanning de medewerker op ieder tijdstip, vanaf iedere willekeurige plek en met ieder willekeurig device, te laten inloggen en veilig, flexibel en gecontroleerd toegang te geven tot zijn persoonlijke werkplek.
• Mocht er toch informatie of bedrijfsinformatie van derde partijen, waarvan de gemeente niet de bronhouder is maar via het platform wordt ontsloten op het device worden opgeslagen dan geldt dat er geen plicht bestaat het eigen device te beveiligen, maar informatie van de organisatie of die van derde partijen daarop wel.
• Voorzieningen als web mail, alsook sociale netwerken en clouddiensten (Dropbox, Gmail, et cetera), zijn door het lage beschermingsniveau (veelal alleen naam en wachtwoord en het ontbreken van versleuteling) niet geschikt voor het delen van vertrouwelijke en geheime informatie.
• Toegang tot vertrouwelijke informatie wordt verleend op basis van multifactor authenticatie.

Dit beleid treedt in werking na vaststelling door het College van B&W. Hiermee komt het oude beleid van de gemeente Oisterwijk te vervallen.

Aldus vastgesteld door het College van B&W van de gemeente,
21 augustus 2018

Bijlage 1 Verklaring kennisname voorwaarden telewerken bij de gemeente Oisterwijk

Ondergetekende

Naam :

Geboortedatum :

Werkzaam bij : de gemeente Oisterwijk

Verklaart hierbij kennis te hebben genomen van de navolgende gebruikersvoorwaarden voor telewerken bij de gemeente Oisterwijk

a. een privé-device ter voorkoming van hacken voorzien van een:
- Antivirus programma
- personal firewall
- screensaver beveiligd met een wachtwoord
- van de laatste beschikbare update voor besturingssysteem en applicaties.

b. Bekend te zijn met het feit dat het is verboden om bedrijfsinformatie lokaal op de privé-device op te slaan zodat datalekken voorkomen kunnen worden.
c. Bekend te zijn met het feit dat hij/zij als een goede gebruiker dient te zorgen voor de aan hem/haar door de gemeente Oisterwijk beschikbaar gestelde apparatuur (zoals device en token), en zelf geen applicaties te installeren zonder toestemming van de beheerorganisatie.
d. Het verboden is om vanuit een internetcafé of via een onbeveiligde (openbare) draadloze verbinding te telewerken zodat datalekken voorkomen kunnen worden.

Oisterwijk, d.d.
Tekenen voor gezien,

(handtekening)