

# **TELEWERKBELEID**

**Een van de producten van de operationele variant van de Baseline  
Informatiebeveiliging Nederlandse Gemeenten (BIG)**



## Colofon

### **Naam document**

Telewerkbeleid

### **Versienummer**

1.0

### **Versiedatum**

April 2014

### **Versiebeheer**

Het beheer van dit document berust bij de Informatiebeveiligingsdienst voor gemeenten (IBD).

### **Copyright**

© 2014 Kwaliteitsinstituut Nederlandse Gemeenten (KING).

Alle rechten voorbehouden. Verveelvoudiging, verspreiding en gebruik van deze uitgave voor het doel zoals vermeld in deze uitgave is met bronvermelding toegestaan voor alle gemeenten en overheidsorganisaties.

Voor commerciële organisaties wordt hierbij toestemming verleend om dit document te bekijken, af te drukken, te verspreiden en te gebruiken onder de hiernavolgende voorwaarden:

1. KING wordt als bron vermeld;
2. het document en de inhoud mogen commercieel niet geëxploiteerd worden;
3. publicaties of informatie waarvan de intellectuele eigendomsrechten niet bij de verstrekker berusten, blijven onderworpen aan de beperkingen opgelegd door KING;
4. ieder kopie van dit document, of een gedeelte daarvan, dient te zijn voorzien van de in deze paragraaf vermelde mededeling.

### **Rechten en vrijwaring**

KING is zich bewust van haar verantwoordelijkheid een zo betrouwbaar mogelijke uitgave te verzorgen. Niettemin kan KING geen aansprakelijkheid aanvaarden voor eventueel in deze uitgave voorkomende onjuistheden, onvolledigheden of nalatigheden. KING aanvaardt ook geen aansprakelijkheid voor enig gebruik van voorliggende uitgave of schade ontstaan door de inhoud van de uitgave of door de toepassing ervan.

### **Met dank aan**

De expertgroep en de reviewgemeenten die hebben bijgedragen aan het vervaardigen van dit product.

### **In samenwerking met**

De producten van de operationele variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) worden vervaardigd in samenwerking met:

## Voorwoord

De IBD is een gezamenlijk initiatief van de Vereniging van Nederlandse Gemeenten (VNG) en het Kwaliteitsinstituut Nederlandse Gemeenten (KING) en actief sinds 1 januari 2013. Aanleiding voor de oprichting van de IBD vormen enerzijds de leerpunten uit een aantal grote incidenten op informatiebeveiligingsvlak en anderzijds de visie Digitale Overheid 2017.

De IBD is er voor alle gemeenten en richt zich op bewustwording en concrete ondersteuning om gemeenten te helpen hun informatiebeveiliging naar een hoger plan te tillen.

### De IBD heeft drie doelen:

1. het preventief en structureel ondersteunen van gemeenten bij het opbouwen en onderhouden van bewustzijn als het gaat om informatiebeveiliging.
2. het leveren van integrale coördinatie en concrete ondersteuning op gemeente specifieke aspecten in geval van incidenten en crisissituaties op het vlak van informatiebeveiliging.
3. het bieden van gerichte projectmatige ondersteuning op deelgebieden om informatiebeveiliging in de praktijk van alle dag naar een hoger plan te tillen. De ondersteuning die de IBD biedt bij het ICT-Beveiligingsassessment DigiD is een voorbeeld van een dergelijk project.

### Hoe realiseert de IBD haar doelen?

Om invulling te kunnen geven aan haar doelen is door de IBD op basis van de Baseline Informatiebeveiliging Rijksdienst (BIR) een vertaalslag gemaakt naar een baseline voor de gemeentelijke markt. Deze Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) betreft twee varianten, een Strategische- én een Tactische Baseline. Beide varianten van de BIG zijn beschikbaar voor alle gemeenten op de website en community van de IBD, zodat door iedere gemeente tot implementatie van de BIG kan worden overgegaan. Bestuur en management hebben met deze baseline een instrument in handen waarmee zij in staat zijn om te meten of de organisatie 'in control' is op het gebied van informatiebeveiliging. Om de implementatie van de Strategische en Tactische Baseline te ondersteunen, zijn door de IBD in samenwerking met de Taskforce Bestuur en Informatieveiligheid Dienstverlening producten ontwikkeld op operationeel niveau. Dit heeft een productenportfolio opgeleverd, genaamd de Operationele Baseline Nederlandse Gemeenten. Onderhavig product is er één van.

Naast een productenportfolio, heeft de IBD voor gemeenten ook een dienstenportfolio ontwikkeld. Voor een volledig overzicht van het producten- en dienstenportfolio, kunt u terecht op de website van de IBD.

De gemeente is zelf verantwoordelijk voor het opstellen en/of uitvoeren en/of handhaven van de regels. Hierbij geldt:

- Er is wetgeving waar altijd aan voldaan moet worden, zoals niet uitputtend: GBA, SUWI, BAG, PUN en WBP, maar ook de archiefwet.
- Er is een gemeenschappelijk normenkader als basis: de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).
- De gemeente stelt dit normenkader vast, waarbij er ruimte is in de naleving van dat kader voor afweging en prioritering op basis van het 'pas toe of leg uit' principe.

## Leeswijzer

Dit product maakt onderdeel uit van de operationele variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

### Doel

Deze aanwijzing is geschreven om vanuit verschillende gezichtspunten de risico's en oplossingen weer te geven die gemeenten kunnen inzetten rondom telewerken.

### Doelgroep

Dit document is van belang voor het gemeentebestuur (voor het beleid) en ICT-beheer.

### Relatie met overige producten

- Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)
  - o Strategische Baseline Informatiebeveiliging Nederlandse Gemeenten
  - o Tactische Baseline Informatiebeveiliging Nederlandse Gemeenten
- Het voorbeeld Informatiebeveiligingsbeleid van de gemeente, §3.1 en §7.3

### Maatregelen tactische variant Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

Maatregel 11.3.2	Onbeheerde gebruikersapparatuur
Maatregel 11.3.3	Clear desk en clear screen
Maatregel 11.5.5	Time-out van sessies
Maatregel 11.7.1	Draagbare computers en communicatievoorzieningen
Maatregel 11.7.2	Telewerken

## **Inhoud**

<b>1</b>	<b>Inleiding</b>	<b>6</b>
1.1	Raakvlakken	7
<b>2</b>	<b>Telewerken</b>	<b>9</b>
2.1	Bedreigingen en maatregelen	9
	<b>Bijlage 1: Gebruiksvoorwaarden voor telewerken gemeente &lt;naam gemeente&gt;</b>	<b>21</b>
	<b>Bijlage 2: Telewerk aanwijzing gemeente &lt;naam gemeente&gt;</b>	<b>22</b>
	<b>Bijlage 3: Definities</b>	<b>25</b>
	<b>Bijlage 4: Literatuur/bronnen</b>	<b>27</b>

## **1 Inleiding**

De Baseline Informatiebeveiliging voor Gemeenten (BIG) heeft maatregelen beschreven die te maken hebben met het werken op afstand (telewerken), zie hiervoor paragraaf 3.1, 6.1 en 7.3 in het voorbeeld gemeentelijk informatiebeveiligingsbeleid en paragraaf 11.7.2 van de BIG.

Dit document geeft algemene aanwijzingen over het werken op afstand. Tenslotte is er aanvullend een gemeentelijk telewerkbeleid. Ten behoeve van de beveiliging van gemeentelijke systemen en de informatie binnen deze gemeentelijke systemen, is dit beleid er op gericht hoe met telewerken omgegaan moet worden. Het kan hierbij ook gaan om bedrijfsinformatie van derde partijen, waarvan de gemeente niet de bronhouder is, indien deze via het gemeentelijk platform wordt ontsloten en beschikbaar gesteld wordt aan de telewerker. Aan informatie kunnen ook wettelijke vereisten gesteld zijn. Bijvoorbeeld het telewerken in relatie tot de GBA.<sup>1</sup>

Er zijn verschillende definities van telewerken<sup>2</sup> in omloop en er worden termen met vergelijkbare betekenissen door elkaar gebruikt. Voorbeelden hiervan zijn 'het nieuwe werken', 'e-werken' en 'flexwerken'. In dit document wordt voor telewerken de volgende definitie gehanteerd 'onafhankelijk van tijd en plaats werken met behulp van informatie- en communicatietechnologie (ICT), buiten de vaste werkomgeving' van de gemeente.

De doelstelling van telewerken kan voor de gemeenten divers zijn. Bijvoorbeeld: verbeteren van de productiviteit/efficiency, kostenbesparing door minder kantoorruimte, flexibiliteit in werktijden, minder reistijd en betere balans tussen werk en privé.

Voor het uitvoeren van werkzaamheden hebben telewerkers toegang tot informatie en informatiesystemen die onder de verantwoordelijkheid vallen van de gemeente waarvoor zij werkzaam zijn. Dit kan ook informatie zijn uit externe bronnen, zoals SUWI<sup>3</sup>, RDW<sup>4</sup>, UWV<sup>5</sup>, DUO<sup>6</sup>, GBA-V<sup>7</sup>, SVB<sup>8</sup>, Kadaster, Belastingdienst Toeslagen et cetera, waarover gemeenten de beschikking hebben of rechtstreeks toegang toe hebben. Deze gegevens, waarvan de gemeente geen bronhouder is, kan de gemeente via een eigen voorziening aan de medewerker beschikbaar stellen of via een ketenvoorziening. Het ontsluiten van deze informatie buiten de beheersbare gemeentelijke bedrijfsomgeving leidt tot extra beveiligingsrisico's. Deze risico's kan de gemeente verkleinen door beveiligingsmaatregelen te treffen.<sup>9</sup>

Er is een toename van telewerken binnen de gemeenten. Er zijn steeds meer situaties waar de medewerker van de gemeente buiten de locatie van de gemeente werkzaamheden heeft, bijvoorbeeld voor werkzaamheden binnen het sociale domein zoals wijkteams maar ook voor

---

<sup>1</sup> [http://www.bprbz.nl/BRP/Informatiebank/Vraag\\_en\\_antwoord/BRP\\_GBA#faq-3](http://www.bprbz.nl/BRP/Informatiebank/Vraag_en_antwoord/BRP_GBA#faq-3)

<sup>2</sup> Definitie telewerken volgens De Van Dale Grote woordenboeken hedendaags Nederlands betekent telewerken: thuis werken met behulp van een computeraansluiting met het bedrijf.

<sup>3</sup> De wet Structuur Uitvoering Werk en Inkomen (SUWI)

<sup>4</sup> Rijksdienst voor het Wegverkeer (RDW). De Wegenverkeerswet 1994 spreekt van een Dienst Wegverkeer.

<sup>5</sup> Het Uitvoeringsinstituut Werknemersverzekeringen (UWV)

<sup>6</sup> Dienst Uitvoering Onderwijs (DUO)

<sup>7</sup> Gemeentelijke Basisadministratie Persoonsgegevens Verstrekkingvoorziening (GBA-V)

<sup>8</sup> De Sociale Verzekeringsbank (SVB)

<sup>9</sup> Het kan dus zijn dat gegevens slechts "ter beschikking gesteld" worden aan een gemeente (of specifieke ambtenaar van een gemeente voor een specifieke taak). De voorwaarden waaronder de gegevens ter beschikking gesteld worden blijven te allen tijde van kracht (wel of geen telewerken). Dit kunnen dus voorwaarden zijn die van invloed zijn op de mogelijke beveiligingsmaatregelen. Bijvoorbeeld alleen apparaten toestaan die eigendom zijn van de gemeente in plaats van privé-eigendom.

handhavingstaken. Bij het telewerken wordt ook steeds vaker gebruik gemaakt van mobiele apparaten zoals smartphones, tablets en laptops. Deze aanwijzing is geschreven om vanuit verschillende gezichtspunten de risico's en oplossingen weer te geven die gemeenten kunnen inzetten bij de keuzes met betrekking tot telewerken. Het maakt voor deze aanwijzing niet uit of het een door de gemeente verstrekt werkstation of mobiel apparaat is, of een privé werkstation, immers op een werkstation kan in meer of mindere mate data van de gemeente staan. Los van het feit of het mobiele apparaat fysiek kan zoekraken, de gemeente is in alle gevallen verantwoordelijk voor deze data.

## 1.1 Raakvlakken

Overige raakvlakken die telewerken hebben met de BIG zijn:

- Informatiebeveiligingsbeleid van de gemeente
- Patch management voor gemeenten
- Handreiking dataclassificatie
- Anti-malware beleid
- Toegangsbeleid
- Mobile Device Management
- Mobiele gegevensdragers
- Encryptie beleid (PKI)
- Procedure afvoer ICT-middelen
- ICT-beheer
- Gedragsregels gebruikers

## 1.2 Aanwijzing voor gebruik

Deze handleiding is geschreven om informatiebeveiligingsmaatregelen met betrekking tot telewerken uit te werken en daarbij aanwijzingen te geven voor het beleid rondom telewerken voor gemeenten.

De gemeentelijke beleidsregels met betrekking tot telewerken zijn:<sup>10</sup>

- Voor werken op afstand is een thuiswerkomgeving beschikbaar of er wordt gebruik gemaakt van een mobiel apparaat zoals een laptop, een tablet of een smartphone. Toegang tot vertrouwelijke informatie wordt verleend op basis van multifactor authenticatie.
- Onbeheerde apparatuur (privé-apparaten of de 'open laptop') kan gebruik maken van draadloze toegangspunten (wifi). Deze zijn logisch gescheiden van het gemeentelijke bedrijfsnetwerk.
- Mobiele bedrijfsapplicaties worden bij voorkeur zo aangeboden dat er geen gemeentelijke informatie wordt opgeslagen op het mobiele apparaat ('zero footprint'). Gemeentelijke informatie en bedrijfsinformatie van derde partijen, waar de gemeente niet de bronhouder van is, maar via het gemeentelijk platform wordt ontsloten dient te worden versleuteld bij transport en opslag, conform classificatie eisen.<sup>11</sup>
- Voorzieningen als webmail, als ook sociale netwerken en Cloud-diensten (Dropbox, Gmail, etc.) zijn door het lage beschermingsniveau (veelal alleen naam en wachtwoord, het ontbreken van versleuteling en ontbreken van controleerbare beveiliging) niet geschikt voor het delen van vertrouwelijke en geheime gemeentelijke informatie.

<sup>10</sup> Zie ook het algemene informatiebeveiligingsbeleid

<sup>11</sup> Zie hiervoor ook het operationele product 'Handreiking dataclassificatie' van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

# INFORMATIE BEVEILIGINGS DIENST

- Beveiligingsmaatregelen hebben betrekking op zowel door de gemeente verstrekte middelen als privé-apparatuur ('bring your own device' (BYOD)). Op privé-apparatuur waarmee verbinding wordt gemaakt met het gemeentelijke netwerk is de gemeente bevoegd om beveiligingsinstellingen af te dwingen. Dit betreft onder meer: controle op wachtwoord, encryptie, aanwezigheid van malware, et cetera. Het gebruik van privé-apparatuur waarop beveiligingsinstellingen zijn verwijderd ('jail break', 'rooted device') is niet toegestaan.
- Op verzoek van de gemeente dienen medewerkers de installatie van software om bovenstaande beleidsregel te handhaven toe te staan (denk bijvoorbeeld aan 'mobile device management software'). De beveiligingsinstellingen, zoals bedoeld in bovenstaande regel, zijn uitsluitend bedoeld ter bescherming van gemeentelijke informatie en integriteit van het gemeentelijke netwerk.
- In geval van dringende redenen kunnen noodmaatregelen worden getroffen, zoals wissen van apparatuur op afstand. Deze noodmaatregelen kunnen, voor zover dit noodzakelijk is, betrekking hebben op privé-middelen en privé-bestanden. Hiervoor wordt een regeling ontwikkeld.
- Voor het werken op afstand en het gebruik van privé-middelen worden nadere regels opgesteld. Echter, de medewerker is gehouden aan regels zoals:
  - Illegale software mag niet worden gebruikt voor de uitvoering van het werk.
  - Er bestaat geen plicht de eigen computer te beveiligen, maar de gemeentelijke informatie daarop wel. Daarmee kan de gemeente regels opstellen die genomen moeten worden om gemeentelijke informatie op een privé-computer te beschermen.
  - Het verbod op ongewenst gebruik in de (fysieke) kantooromgeving geldt ook als dat via de eigen computer plaatsvindt.



## 2 Telewerken

Beleid, operationele plannen en procedures voor telewerken dienen te worden ontwikkeld en geïmplementeerd binnen de gemeente:

1. Er wordt beleid met gedragsregels en een geschikte implementatie van de techniek opgesteld ten aanzien van telewerken.
2. Er wordt beleid vastgesteld met daarin de uitwerking van welke systemen niet, en welke systemen wel vanuit de thuiswerkplek of andere apparaten mogen worden geraadpleegd. Dit beleid wordt bij voorkeur ondersteund door een MDM-oplossing (Mobile Device Management).
3. 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.  
Voor printen in niet vertrouwde omgevingen vindt een risicoafweging plaats.

### 2.1 Bedreigingen en maatregelen

De bedreigingen en maatregelen bij telewerken kan men indelen naar de schakels van de telewerkketen tussen medewerker en de ICT-infrastructuur van de gemeente, namelijk<sup>12</sup>:

- De telewerklocatie
- De telewerkvoorziening zoals een desktop, laptop, tablet of smartphone. In het vervolg aangeduid met 'apparaat'.
- De verbinding tussen het apparaat en de ICT-infrastructuur van de gemeente
- De systemen die door de telewerker benaderd kunnen worden
- De informatie die aan de telewerker beschikbaar wordt gesteld
- De telewerker zelf

#### De telewerklocatie

Telewerken vindt plaats vanaf een locatie buiten de gemeentelijke organisatie en de grootste bedreiging is dat (vertrouwelijke) informatie wordt onderschept. Deze omgeving valt voor een deel buiten de invloedssfeer van de gemeente, daarom is voor de beveiliging van een telewerkplek een mix van technische, procedurele en organisatorische maatregelen nodig. De gemeente is bevoegd om eisen te stellen als het een vaste telewerklocatie betreft, bijvoorbeeld thuis.

Indien een medewerker op een openbare locatie telewerkt, bestaat de kans dat een buitenstaander gevoelige informatie vanaf het beeldscherm leest of een telefoongesprek afluistert. De menselijke nieuwsgierigheid is een factor waar rekening mee moet worden gehouden. Daarnaast kan het mobiele apparaat van de telewerker zoekraken. Door verlies of diefstal van het mobiele apparaat bestaat de mogelijkheid dat de daarop opgeslagen informatie in handen komt van een buitenstaander.

Gebruikt een telewerker een computer van een ander, zoals in een bibliotheek of gemeentehuis of van een vriend of de buurman, dan bestaat de mogelijkheid dat de volgende gebruiker van deze computer, de in de cache opgeslagen informatie van de vorige sessie kan inzien.

---

<sup>12</sup> Voor de concrete invulling van de maatregelen kan gebruik gemaakt worden van de beveiligingspatronen die door de De Nederlandse Overheid Referentie Architectuur (NORA) zijn opgesteld (<http://noraonline.nl/wiki/Beveiligingspatronen>). Een voorbeeld is het patroon voor externe koppelvlakken.

De gemeente kan weinig invloed uitoefenen op de omgeving van een telewerklocatie. Een telewerklocatie is een werkplek buiten de gemeentelijke organisatie en daarmee buiten bereik van de directe beheerorganisatie van de gemeente.

Hieronder een overzicht van de belangrijkste risico's met betrekking tot de telewerklocatie en welke maatregelen uit de BIG kunnen worden genomen om het risico te verlagen.

<b>Risico:</b>	Onbevoegden kunnen gevoelige informatie vanaf het beeldscherm meelezen
<b>Maatregel:</b>	<ul style="list-style-type: none"><li>• Specifiek aandacht voor deze kwestie in bewustwordingscampagnes.</li><li>• Vaststellen en implementeren gebruiksvoorwaarden voor telewerken met daarin onder andere:<ul style="list-style-type: none"><li>○ Op welke locaties de telewerker mag telewerken. Zo kan men bijvoorbeeld verbieden om vanuit een internetcafé of via een onbeveiligde (openbare) draadloze verbinding te telewerken.</li></ul></li><li>• Clear screen-beleid voor ICT-voorzieningen:<ul style="list-style-type: none"><li>○ Schermbeveiligingsprogrammatuur (een screensaver) maakt na een periode van maximaal 15 minuten van inactiviteit alle informatie op het beeldscherm onleesbaar en ontoegankelijk.</li><li>○ Schermbeveiliging wordt automatisch geactiveerd bij het verwijderen van een token (indien aanwezig).</li><li>○ De gebruiker vergrendelt de werkplek tijdens afwezigheid.</li></ul></li><li>• Als additionele maatregel op de BIG kan men gebruik maken van een privacyscherm. Een privacyscherm beschermt tegen meekijken op het apparaat, de gebruiker moet namelijk recht voor het beeldscherm zitten om de gegevens te kunnen bekijken.</li></ul>

<b>Risico:</b>	Onbevoegden kunnen gevoelige informatie onderscheppen door telefoongesprekken af te luisteren.
<b>Maatregel:</b>	<ul style="list-style-type: none"><li>• Specifiek aandacht voor deze kwestie in bewustwordingscampagnes.</li><li>• Vaststellen en implementeren gebruiksvoorwaarden voor telewerken met daarin onder andere:<ul style="list-style-type: none"><li>○ Beperk het uitwisselen van gevoelige informatie in openbare locaties via de telefoon tot een minimum.</li></ul></li></ul>

<b>Risico:</b>	Informatie in handen van een buitenstaander door verlies of diefstal van papier of mobiele gegevensdragers. <sup>13</sup>
<b>Maatregel:</b>	<ul style="list-style-type: none"><li>• Specifiek aandacht voor deze kwestie in bewustwordingscampagnes.</li><li>• Vaststellen en implementeren gebruiksvoorwaarden voor telewerken met daarin onder andere:<ul style="list-style-type: none"><li>○ Verlies of diefstal van mobiele gegevensdragers met vertrouwelijke informatie moet direct als beveiligingsincident worden gemeld. Deze melding moet minimaal altijd worden gedaan aan de CISO, of verantwoordelijke informatiebeveiliging van de betreffende gemeente.</li></ul></li><li>• Clear desk-beleid voor papier en verwijderbare opslagmedia:<ul style="list-style-type: none"><li>○ De gebruiker mag geen gevoelige informatie op het bureau laten</li></ul></li></ul>

<sup>13</sup> Zie hiervoor ook het operationele product 'Mobiele gegevensdragers' van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

liggen. Deze informatie moet altijd worden opgeborgen in een afsluitbare opbergmogelijkheid (kast, locker, bureau of kamer).

- Het printen in niet vertrouwde omgevingen wordt afgeraden, maar als het niet anders kan wordt voor het printen door de telewerker een risicoafweging gemaakt. Na het printen dient de telewerker de documenten meteen bij de printer op te halen.

## Het apparaat zoals een desktop, laptop, tablet of smartphone

Apparaten die voor telewerken worden gebruikt kunnen eigendom van de telewerker of de gemeente zijn of van iemand anders. Indien de telewerker een door de gemeente beheerd apparaat ter beschikking heeft, kan de gemeente bepalen welke beveiligingsmaatregelen zij hierop aanbrengt. Daarmee kan een gemeente de risico's voor het apparaat grotendeels afdekken.<sup>14</sup> Voor een privé-apparaat is dat anders. Dit apparaat is, over het algemeen, niet in beheer bij de gemeente. De gemeente is wel bevoegd om beveiligingsinstellingen af te dwingen als privé-apparaten (ook) zakelijk wordt gebruikt ('bring your own device'). Dit betreft onder meer: controle op wachtwoord, encryptie, aanwezigheid van malware, et cetera. Op verzoek van de gemeente dienen medewerkers de installatie van software om bovenstaande beveiligingsinstellingen te handhaven toe te staan (denk bijvoorbeeld aan 'mobile device management software'). Apparaten van andere zijn niet in beheer bij de gemeente en daardoor kunnen de risico's aanmerkelijk groter zijn dan bij een door de gemeente beheerd apparaat.

De grootste bedreigingen met betrekking tot het apparaat zijn: manipulatie van gegevens of onbevoegd inzien, een malware besmetting, zoekraken van het apparaat en gebruikers zijn zich vaak niet bewust van de risico's die het gebruik van (mobiele) apparaten met zich meebrengen.

Mogelijke oorzaken zijn:

- Geen vastgesteld gemeentelijk beleid over welke gegevens op het apparaat mogen staan, geen dataclassificatie beleidsregels
- Malware op het apparaat
- Klikken op links in mail en webpagina's die niet vertrouwd zijn
- Verbinden via onveilige open netwerken, waar men kan worden aangevallen door derden
- Man in the middle attack<sup>15</sup>
- Niet vergrendelen van het apparaat
- Geen versleuteling, terwijl dat wel nodig is
- Diefstal van het apparaat
- 'Rooten' of 'jailbreaken' van het apparaat<sup>16</sup>
- Verlies (onopzettelijk) van het apparaat
- Bedrijfsinformatie wordt (onversleuteld) op mobiele gegevensdragers opgeslagen
- Ongeautoriseerde toegang tot, of technische storingen op het apparaat. Ongeautoriseerde toegang tot het apparaat kan lokaal of op afstand plaatsvinden. In het eerste geval spelen ook de risico's rondom de werklocatie een rol
- De telewerker heeft op zijn privé-apparaat alle rechten en kan hierop willekeurige software installeren

<sup>14</sup> Zie hiervoor ook het operationele product 'Mobile Device Management' van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

<sup>15</sup> <http://nl.wikipedia.org/wiki/Man-in-the-middle>

<sup>16</sup> Jailbreak is het mogelijk maken van het draaien van niet goedgekeurde apps op een iOS apparaat, waardoor ook malware gedraaid kan worden. Rooten is het proces dat het mogelijk maakt men meer rechten krijgt op het apparaat (android) en daardoor het complete besturings systeem te wijzigen of te vervangen, en daarmee malware introduceren en gemeentelijke beveiligingsinstellingen te omzeilen.

# INFORMATIE BEVEILIGINGS DIENST

- Ongeautoriseerd, te laat, onjuist of onvolledig installeren van updates op het apparaat.<sup>17</sup> Deze kwetsbaarheid neemt toe naarmate de organisatie minder invloed heeft op het beheer van het apparaat.

De mogelijke gevolgen zijn:

- Installatie van kwaadaardige software die gegevens steelt, zichzelf toegang verschaft, maar ook zichzelf verspreidt over andere gemeentelijke systemen.
- Mogelijk inzien gegevens door onbevoegden, kopiëren, wijzigen en vernietigen van gegevens.
- Het apparaat moet vervangen worden voor een nieuw apparaat.
- Toegang tot gemeentelijke systemen via het apparaat.

Hieronder een overzicht van de belangrijkste risico's en welke maatregelen kunnen worden genomen om deze risico's te verlagen.

<b>Risico:</b>	Informatie in handen van een buitenstaander (manipulatie van gegevens of onbevoegd inzien).
<b>Maatregel:</b>	<ul style="list-style-type: none"><li>• Specifiek aandacht voor deze kwestie in bewustwordingscampagnes.</li><li>• Alle apparaten, zowel van de gemeente of privé, waarop gemeentelijke gegevens kunnen staan worden bij voorkeur beheerd met een MDM-tool<sup>18</sup>, zodat het beveiligingsbeleid op het apparaat kan worden afgedwongen (technisch afdwingen van het beleid).</li><li>• Op een door de gemeente beheerd apparaat zijn beveiligingsmaatregelen technisch af te dwingen door de gemeente. Deze maatregelen omvatten:<ul style="list-style-type: none"><li>○ Welke software op het apparaat geïnstalleerd wordt, inclusief beveiligingssoftware zoals:<ul style="list-style-type: none"><li>• Up-to-date virusscanner</li><li>• Up-to-date personal firewall</li><li>• Up-to-date anti malware tool</li><li>• Up-to-date besturingssysteem en applicaties (zie hiervoor patchmanagement)</li></ul></li><li>○ Welke rechten de telewerker op het apparaat krijgt</li><li>○ Dat de telewerker met een gebruikersnaam en wachtwoord inlogt, eventueel ondersteund door een certificaat, waarmee voorkomen wordt dat een derde ongemerkt toegang krijgt tot de informatie die op het apparaat aanwezig is.</li></ul></li><li>• Vaststellen en implementeren gebruiksvoorwaarden voor telewerken met daarin onder andere:<ul style="list-style-type: none"><li>○ Dat geen bedrijfsinformatie op mobiele gegevensdragers mag worden opgeslagen. Als het niet anders kan dient deze bedrijfsinformatie te worden versleuteld.<sup>19</sup></li><li>○ De telewerker zorgt als een goede huisvader voor het ,aan hem door de gemeente beschikbaar gestelde, apparaat en installeert zelf geen applicaties, zonder toestemming van de beheerorganisatie.</li></ul></li></ul>

<sup>17</sup> Zie hiervoor ook het operationele product 'Patch management voor gemeenten' van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

<sup>18</sup> Zie hiervoor ook het operationele product 'Mobile Device Management' van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

<sup>19</sup> Zie hiervoor ook het operationele product 'Mobiele gegevensdragers' van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

- Dat geen bedrijfsinformatie lokaal op het privé-apparaat wordt opgeslagen, om zo de kans te beperken dat het via spyware uitgelezen kan worden.<sup>20</sup>
- Clear screen-beleid voor ICT-voorzieningen:
  - Schermbeveiligingsprogrammatuur (een screensaver) maakt na een periode van maximaal 15 minuten van inactiviteit alle informatie op het beeldscherm onleesbaar en ontoegankelijk.
  - Schermbeveiliging wordt automatisch geactiveerd bij het verwijderen van een token (indien aanwezig).
  - De gebruiker vergrendelt de werkplek tijdens afwezigheid.
- Uitzetten van services die niet direct nodig zijn (hardening van het apparaat<sup>21</sup>)
- Het apparaat is zo ingericht dat geen bedrijfsinformatie wordt opgeslagen ('zero footprint'). Voor het geval dat zero footprint (nog) niet realiseerbaar is, of functioneel onwenselijk is, wordt de toegang tot het apparaat beschermd door middel van een wachtwoord en is apparaat versleuteling geïmplementeerd (conform classificatie eisen). In ieder geval beveiligde opslag van gemeentelijke informatie en bedrijfsinformatie van derde partijen, waar de gemeente niet de bronhouder van is, maar via het gemeentelijk platform wordt ontsloten. Als deze informatie al wordt toegestaan op het apparaat.

Een alternatief om decentrale opslag van gemeentelijke gegevens te voorkomen is Virtuele Desktop Infrastructuur (VDI).<sup>22</sup> Het stelt wel extra eisen aan de serveromgeving en het netwerk, maar voor het beheer betekent de virtuele desktop vaak een efficiëncyslag. 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 apparaat inloggen, veilig, flexibel en gecontroleerd toegang te geven tot zijn persoonlijke werkplek.

**Risico:** Het apparaat kan een malware besmetting oplopen en daarmee mogelijk de gemeente infecteren. Het apparaat wordt door hackers als aanvalsvector gebruikt.

**Maatregel:**

- Specifiek aandacht voor deze kwestie in bewustwordingscampagnes
- Vaststellen en implementeren gebruiksvoorwaarden voor telewerken met daarin onder andere:
  - Dat geen gebruik wordt gemaakt van niet vertrouwde netwerken
  - Dat niet op links in mail en webpagina's wordt geklikt die niet vertrouwd worden
  - Het privé-apparaat dat wordt gebruikt bij het telewerken moet zijn voorzien van:

<sup>20</sup> <http://nl.wikipedia.org/wiki/Spyware>

<sup>21</sup> Zie hiervoor ook het operationele product 'Hardening beleid' van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

<sup>22</sup> Deze infrastructuur laat toe om op afstand (bijvoorbeeld via het internet) en met een eigen apparaat, te werken op een virtueel besturingssysteem dat niet op het lokale apparaat, maar op de server draait. Om met een virtuele desktop te werken, moet een VDI client op het apparaat geïnstalleerd zijn die een veilige verbinding maakt met het virtuele besturingssysteem op de server.

- Up to date virusscanner
  - Personal firewall<sup>23</sup>
  - Anti malware tool<sup>24</sup>
  - Screensaver beveiligd met een wachtwoord
  - Up-to-date besturingssysteem en applicaties<sup>25</sup>
- Het apparaat dat een verbinding met de ICT-infrastructuur van de gemeente wil opzetten wordt gecontroleerd of deze voorzien is van een up-to-date virusscanner en een firewall. Indien het apparaat niet of onvoldoende is beveiligd (bijvoorbeeld virusdefinities niet up-to-date), kan de toegang tot de ICT-infrastructuur van de gemeente worden geweigerd. Door het uitvoeren van dit soort controles wordt voorkomen dat gemeentelijke systemen geïnfecteerd raken met malware. Om de hulpmiddelen te bieden waarmee het apparaat weer beveiligd kan worden, wordt het apparaat in een quarantainenetwerk geplaatst.<sup>26</sup> Hierdoor krijgt de telewerker slechts toegang tot een beperkt aantal websites, namelijk die van virusscanners, firewalls, Windows Update, et cetera.
- Alle apparaten, zowel van de gemeente of privé, waarop gemeentelijke gegevens kunnen staan worden bij voorkeur beheerd met een MDM-tool<sup>27</sup>, zodat het beveiligingsbeleid op het apparaat kan worden afgedwongen (technisch afdwingen van het beleid)
- Uitzetten van services die niet direct nodig zijn (hardening van het apparaat<sup>28</sup>)

**Risico:** Informatie in handen van een buitenstaander door verlies of diefstal van het apparaat.

**Maatregel:**

- Specifiek aandacht voor deze kwestie in bewustwordingscampagnes.
- Het apparaat is zo ingericht dat geen bedrijfsinformatie wordt opgeslagen ('zero footprint'). Voor het geval dat zero footprint (nog) niet realiseerbaar is, of functioneel onwenselijk is, wordt de toegang tot het apparaat beschermd door middel van een wachtwoord en is apparaat versleuteling geïmplementeerd (conform classificatie eisen). In ieder geval beveiligde opslag van gemeentelijke informatie en bedrijfsinformatie van derde partijen, waar de gemeente niet de bronhouder van is, maar via het gemeentelijk platform wordt ontsloten. Als deze informatie al wordt toegestaan op het apparaat.

<sup>23</sup> [http://en.wikipedia.org/wiki/Personal\\_firewall](http://en.wikipedia.org/wiki/Personal_firewall)

<sup>24</sup> Zie hiervoor ook het operationele product 'Antimalware beleid' van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

<sup>25</sup> Zie hiervoor ook het operationele product 'Patch management voor gemeenten' van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

<sup>26</sup> Deze oplossing biedt beveiliging tegen het feit dat 'onbedoeld' configuratie instellingen van het apparaat zijn gewijzigd en deze niet zijn hertseld voordat een verbinding met de de ICT-infrastructuur van de gemeente wordt opgezet. Een telewerker kan bijvoorbeeld antivirussoftware uitschakelen, terwijl deze software een vereiste is voor een netwerkverbinding. De computerconfiguraties kunnen worden gecontroleerd en zo nodig worden gecorrigeerd voordat er toegang tot het netwerk wordt verleend. Wanneer de configuratie van het apparaat overeenkomt met het netwerkbeleid van de gemeente, worden de quarantainebeperkingen opgeheven. Een voorbeeld hiervan is de Network Access Quarantine Control (NAQC) oplossing van Microsoft.

<sup>27</sup> Zie hiervoor ook het operationele product 'Mobile Device Management' van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

<sup>28</sup> Zie hiervoor ook het operationele product 'Hardening beleid' van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

Een alternatief om decentrale opslag van gemeentelijke gegevens te voorkomen is Virtuele Desktop Infrastructuur (VDI). Het stelt wel extra eisen aan de serveromgeving en het netwerk maar voor het beheer betekent de virtuele desktop vaak een efficiëncyslag. 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 apparaat in te loggen, veilig, flexibel en gecontroleerd toegang te geven tot zijn persoonlijke werkplek.

- Vaststellen en implementeren gebruiksvoorwaarden voor telewerken met daarin onder andere:
  - Verlies of diefstal van het apparaat moet direct als beveiligingsincident worden gemeld. Deze melding moet minimaal altijd worden gedaan aan de CISO, of verantwoordelijke informatiebeveiliging van de betreffende gemeente.
  - Er dient ook altijd aangifte gedaan te worden bij de politie.
- Na melding van verlies of diefstal worden de communicatiemogelijkheden met de centrale applicaties afgesloten.

## **De verbinding tussen het apparaat en de ICT-infrastructuur van de gemeente**

De grootste bedreiging met betrekking tot de netwerkvoorziening is onbevoegd inzien van gegevens, kopiëren van gegevens, vernietigen en wijzigen van gegevens.

Bij telewerken is vaak sprake van centrale gegevensverwerking en/of -opslag. Hiertoe wordt de centrale informatievoorziening dan wel serveromgeving van de gemeente beschikbaar gesteld via een extern netwerk (meestal het internet) waarop ook de telewerkers aangesloten zijn. De gemeente heeft een bepalende invloed op het beheer van de serveromgeving, maar niet noodzakelijkerwijs op het beheer van het netwerk.

De netwerkverbinding tussen het apparaat en de ICT-infrastructuur van de gemeente (de serveromgeving) kan op verschillende manieren tot stand worden gebracht. Deze netwerkverbindingen kunnen door kwaadwillenden worden afgeluisterd, waardoor deze inzage kunnen krijgen in de informatie die tussen de telewerker en de gemeente wordt uitgewisseld. Gebruikersnaam en wachtwoord kunnen zo worden bemachtigd, waardoor een kwaadwillende zich mogelijk toegang kan verschaffen tot de bedrijfsinformatie waarvoor de gemeente verantwoordelijk is. Dit kan ook bedrijfsinformatie van derde partijen zijn, waarvan de gemeente niet de bronhouder is, indien deze via het gemeentelijk platform wordt ontsloten en beschikbaar gesteld wordt aan de telewerker. Een specifieke bedreiging is de man-in-the-middle (MITM)-aanval.<sup>29</sup>

Ook als een beveiligde verbinding tussen het apparaat en de ICT-infrastructuur van de gemeente uitvalt, is het apparaat vanaf het netwerk te bereiken en bestaat de mogelijkheid dat een kwaadwillende toegang krijgt tot de daarin opgeslagen informatie.

Mogelijke oorzaken zijn:

- Verbinden via onveilige open netwerken, waar men kan worden aangevallen door derden
- Man-in-the-middle-aanval
- Geen versleuteling, terwijl dat wel nodig is

Hieronder een overzicht van de belangrijkste risico's en welke maatregelen uit de BIG kunnen worden genomen om deze risico's te verlagen.

<sup>29</sup> <http://nl.wikipedia.org/wiki/Man-in-the-middle>

<b>Risico:</b>	Informatie in handen van een buitenstaander (manipulatie van gegevens of onbevoegd inzien).
<b>Maatregel:</b>	<ul style="list-style-type: none"><li>• Specifiek aandacht voor deze kwestie in bewustwordingscampagnes.</li><li>• Vaststellen en implementeren gebruiksvoorwaarden voor telewerken met daarin onder andere:<ul style="list-style-type: none"><li>◦ Dat geen gebruik wordt gemaakt van niet vertrouwde netwerken.</li></ul></li><li>• Alle apparaten, zowel van de gemeente of privé, die worden gebruikt om een verbinding met de ICT-infrastructuur van de gemeente op te zetten worden bij voorkeur beheerd met een MDM-tool<sup>30</sup>, zodat het beveiligingsbeleid op het apparaat kan worden afgedwongen (technische afdwingen van het beleid).</li><li>• Het apparaat dat een verbinding met de ICT-infrastructuur van de gemeente wil opzetten wordt gecontroleerd of deze voorzien is van een up-to-date virusscanner en een firewall. Indien het apparaat niet of onvoldoende is beveiligd (bijvoorbeeld virusdefinities niet up-to-date), kan de toegang tot de ICT-infrastructuur van de gemeente worden geweigerd. Het technisch afdwingen van het beleid (ook wel policy enforcement<sup>31</sup> genoemd).</li><li>• Door het uitvoeren van dit soort controles wordt voorkomen dat gemeentelijke systemen geïnfecteerd raken met malware. Om de hulpmiddelen te bieden waarmee het apparaat weer beveiligd kan worden, wordt het apparaat in een quarantainenetwerk<sup>32</sup> geplaatst. Hierdoor krijgt de telewerker slechts toegang tot een beperkt aantal websites, namelijk die van virusscanners, firewalls, Windows Update, et cetera.</li><li>• Door middel van cryptografie wordt de netwerkverbinding tussen het apparaat en de serveromgeving (end-to-end) via versleuteling beveiligd. De technologie om bedrijfsinformatie op het interne netwerk op een veilige manier via het internet te ontsluiten is een VPN<sup>33</sup> (Virtueel Particulier Netwerk), vaak gebaseerd op IPSec<sup>34</sup> (IP Security) of SSL/TLS (Secure Sockets Layer/Transport Layer Security). Deze VPN bestaat uit twee componenten. Een VPN client die op het apparaat van de telewerker wordt geïnstalleerd en de VPN serversoftware die tussen het bedrijfsnetwerk en het internet zit (bijvoorbeeld een network access server (NAS), media gateway of een remote-access server (RAS)). Tussen deze componenten wordt een beveiligde tunnel opgezet waarbinnen versleuteling en authenticatie plaatsvinden. Op deze manier heeft de telewerker op een veilige manier de informatie tot zijn beschikking, zoals</li></ul>

<sup>30</sup> Zie hiervoor ook het operationele product 'Mobile Device Management' van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

<sup>31</sup> [http://www.computerworld.com/s/article/98080/What\\_is\\_policy\\_enforcement\\_and\\_why\\_should\\_we\\_care](http://www.computerworld.com/s/article/98080/What_is_policy_enforcement_and_why_should_we_care)

<sup>32</sup> Deze oplossing biedt beveiliging tegen het feit dat 'onbedoeld' configuratie instellingen van het apparaat zijn gewijzigd en deze niet zijn hersteld voordat een verbinding met de de ICT-infrastructuur van de gemeente wordt opgezet. Een telewerker kan bijvoorbeeld antivirussoftware uitschakelen, terwijl deze software een vereiste is voor een netwerkverbinding. De computerconfiguraties kunnen worden gecontroleerd en zo nodig worden gecorrigeerd voordat er toegang tot het netwerk wordt verleend. Wanneer de configuratie van het apparaat overeenkomt met het netwerkbeleid van de gemeente, worden de quarantainebeperkingen opgeheven. Een voorbeeld hiervan is de Network Access Quarantine Control (NAQC) oplossing van Microsoft.

<sup>33</sup> [http://nl.wikipedia.org/wiki/Virtueel\\_Particulier\\_Netwerk](http://nl.wikipedia.org/wiki/Virtueel_Particulier_Netwerk) en <http://computer.howstuffworks.com/vpn.htm>

<sup>34</sup> <http://nl.wikipedia.org/wiki/IPsec>



hij die ook heeft als hij op het interne bedrijfsnetwerk van de gemeente is aangesloten.

Zowel bij SSL als TLS worden certificaten toegepast. Als de server en de client voorzien zijn van certificaten kan men wederzijdse authenticatie uitvoeren van zowel de server als de client en zo een beveiligde verbinding met de server opzetten.

Dit houdt wel in dat deze client certificaten beheerd moeten worden om misbruik te voorkomen of tijdig waar te nemen.

- Toegang tot de ICT-infrastructuur van de gemeente wordt via verschillende infrastructuren (bijvoorbeeld vast en mobiel internet) ondersteund om complete beschikbaarheid te bereiken.
- Bij een remote desktop sessies geldt dat na maximaal 15 minuten inactiviteit de sessie verbroken wordt.

**Risico:** Het apparaat kan een malware besmetting oplopen en daarmee mogelijk de gemeente infecteren. Het apparaat wordt door hackers als aanvalsvector gebruikt.

**Maatregel:**

- Specifiek aandacht voor deze kwestie in bewustwordingscampagnes.
- Vaststellen en implementeren gebruiksvoorwaarden voor telewerken met daarin onder andere:
  - Dat geen gebruik wordt gemaakt van niet vertrouwde netwerken.
  - Dat niet op links in mail en webpagina's wordt geklikt die niet vertrouwd worden.
  - Het privé-apparaat dat wordt gebruikt bij het telewerken moet zijn voorzien van:
    - Up-to-date virusscanner
    - Personal firewall
    - Anti malware tool
    - Screensaver beveiligd met een wachtwoord
    - Up-to-date besturingssysteem en applicaties
- Het apparaat dat een verbinding met de ICT-infrastructuur van de gemeente wil opzetten wordt gecontroleerd of deze voorzien is van een up-to-date virusscanner en een firewall. Indien het apparaat niet of onvoldoende is beveiligd (bijvoorbeeld virusdefinities niet up-to-date), kan de toegang tot de ICT-infrastructuur van de gemeente worden geweigerd. Door het uitvoeren van dit soort controles wordt voorkomen dat gemeentelijke systemen geïnfecteerd raken met malware. Om de hulpmiddelen te bieden waarmee het apparaat weer beveiligd kan worden, wordt het apparaat in een quarantainenetwerk geplaatst. Hierdoor krijgt de telewerker slechts toegang tot een beperkt aantal websites, namelijk die van virusscanners, firewalls, Windows Update, et cetera.

## **De systemen die door de telewerker benaderd kunnen worden en de informatie die aan de telewerker beschikbaar wordt gesteld**

De meest gebruikte vorm van telewerken is webmail of een webenabled-applicatie met toegang tot interne systemen met bedrijfsinformatie, waarbij gevoelige informatie over het internet wordt verzonden. Een groot voordeel is, dat deze vorm van telewerken overal kan worden gebruikt.

Gegevensverwerking of -opslag op het apparaat vindt plaats op een externe locatie. Hierdoor staan de gegevens bloot aan risico's die samenhangen met de werklocatie en eventuele kwetsbaarheden op het apparaat.

De grootste bedreiging met betrekking tot de toegang tot systemen en gegevens is onbevoegd inzien van gegevens, kopiëren van gegevens, vernietigen en wijzigen van gegevens.

Mogelijke oorzaken zijn:

- De betrouwbaarheid van gegevens op de serveromgeving bedreigd door ongeautoriseerde toegang (inzien en manipulatie) en Denial of Service (DoS)-aanvallen (beschikbaarheid). De impact van deze bedreigingen kan groot zijn omdat dit veel (tele)werkers treft.
- Ongeautoriseerde toegang tot de serveromgeving kan bijvoorbeeld worden veroorzaakt door hacking of via een niet afdoende beveiligd apparaat van telewerkers. Ook kan het zijn dat telewerkers onzorgvuldig omgaan met hun identificatie- en authenticatiemiddelen of derden bewust of onbewust van hun apparaat gebruik laten maken.<sup>35</sup>
- Als de toegang alleen met gebruikersnaam en wachtwoord beveiligd is, loopt men het risico dat dit wachtwoord wordt gekraakt. Hiermee krijgt een kwaadwillende 'gemakkelijk' toegang tot de, voor de telewerker beschikbare, interne bedrijfsinformatie van de gemeente. Dit kan ook bedrijfsinformatie van derde partijen zijn, waarvan de gemeente niet de bronhouder is, indien deze via het gemeentelijk platform wordt ontsloten en beschikbaar gesteld wordt aan de telewerker.

Hieronder een overzicht van de belangrijkste risico's en welke maatregelen uit de BIG kunnen worden genomen om deze risico's te verlagen.

<b>Risico:</b>	Ongeautoriseerde toegang tot de serveromgeving, zowel de systemen als de informatie.
<b>Maatregel:</b>	<ul style="list-style-type: none"><li>• Specifiek aandacht voor deze kwestie in bewustwordingscampagnes.</li><li>• Vaststellen en implementeren gebruiksvoorwaarden voor telewerken met daarin onder andere:<ul style="list-style-type: none"><li>○ Dat geen gebruik wordt gemaakt van niet vertrouwde netwerken.</li><li>○ Dat niet op links in mail en webpagina's wordt geklikt die niet vertrouwd worden.</li></ul></li><li>• Toegang tot gemeente systemen wordt door middel van twee-factor authenticatie beschermd (dus met het apparaat alleen kan geen toegang worden verkregen). Zie de tekst na deze tabel onder het kopje 'Toegang tot informatie' voor een uitgebreidere uitleg.</li><li>• Er wordt waar mogelijk gebruik gemaakt van Role Based Access control.<sup>36</sup> Nadat de telewerker zich heeft geauthenticeerd kan hij, afhankelijk van de functie, geautoriseerd worden voor toegang tot bepaalde applicaties en informatie. Meestal heeft een gemeente al een tool in gebruik voor autorisatie van medewerkers tot applicaties en informatie. Deze kan uitgebreid worden met autorisaties voor medewerkers vanaf een telewerkplek. Het is ook mogelijk om de autorisaties van een medewerker te beperken wanneer hij telewerkt. De hoeveelheid autorisaties van een telewerker kan</li></ul>

<sup>35</sup> Zie hiervoor ook het operationele product 'Toegangsbeleid' van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

<sup>36</sup> [http://nl.wikipedia.org/wiki/Role-based\\_access\\_control](http://nl.wikipedia.org/wiki/Role-based_access_control)

- gerelateerd worden aan het beveiligingsniveau van zijn apparaat.
- Het apparaat dat een verbinding met de ICT-infrastructuur van de gemeente wil opzetten wordt gecontroleerd of deze voorzien is van een up-to-date virusscanner en een firewall. Indien het apparaat niet of onvoldoende is beveiligd (bijvoorbeeld virusdefinities niet up-to-date), kan de toegang tot de ICT-infrastructuur van de gemeente worden geweigerd (afdwingen van het beleid).
  - Extra aandacht moet uitgaan naar het tijdig en volledig intrekken van autorisaties bij uitdiensttreding van telewerkers. Zij hoeven immers geen toegang tot het kantoor te hebben om gebruik te maken van de serveromgeving. Ook als medewerkers van functie veranderen dienen de huidige autorisaties van deze medewerker opnieuw beoordeeld te worden, dit geldt ook voor de mogelijkheid om te mogen telewerken.
  - Implementeren van apparaat authenticatie.
  - Door compartimentering/segmentering van het netwerk, een 'goede' configuratie van de firewall en toepassing van een demilitarized zone (DMZ)<sup>37</sup> kan de toegang van de telewerker tot de informatie, die op een telewerkplek kan worden benaderd, worden beperkt.
  - Door hardening<sup>38</sup> kan de serveromgeving worden afgeschermd van het externe netwerk. Met hardening wordt onder andere bedoeld:
    - Overbodige functies in besturingssystemen uitschakelen en/of van het systeem verwijderen.
    - Zodanige waarden toekennen aan beveiligingsinstellingen dat hiermee de mogelijkheden om een systeem te compromitteren worden verlaagd en een maximale veiligheid ontstaat. Het gaat hierbij ook om het verwijderen van niet gebruikte of onnodige gebruikers accounts, en tevens het wijzigen van standaard wachtwoorden die op sommige systemen aanwezig kunnen zijn.
  - Extra aandacht voor logging en monitoring<sup>39</sup> van toegang tot de serveromgeving. Het doel van deze controle is vaststellen of deze niet misbruikt wordt, goed wordt beheerd en functioneert conform de gestelde eisen. Informatie die minimaal gelogd moet worden, is:
    - Welke apparaten zetten een (VPN) netwerkverbinding op en welke pogingen mislukken.
    - Welke toegangsrechten worden gebruikt of misbruikt voor toegang tot het netwerk van de gemeente. Denk hierbij aan foutieve inlogpogingen, overschrijding van autorisatiebevoegdheden, geweigerde pogingen om toegang te krijgen.
    - Welk netwerkverkeer vindt er plaats tussen het apparaat en het interne netwerk.

## Toegang tot informatie

Voor toegang van de telewerker tot de informatie op het bedrijfsnetwerk van de gemeente wordt aanbevolen multifactor authenticatie toe te passen. Multifactor authenticatie maakt gebruik van het

<sup>37</sup> [http://nl.wikipedia.org/wiki/Demilitarized\\_zone\\_%28informatica%29](http://nl.wikipedia.org/wiki/Demilitarized_zone_%28informatica%29) of [http://en.wikipedia.org/wiki/DMZ\\_%28computing%29](http://en.wikipedia.org/wiki/DMZ_%28computing%29)

<sup>38</sup> Zie hiervoor ook het operationele product 'Hardening beleid' van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

<sup>39</sup> Zie hiervoor ook het operationele product 'Aanwijzingen logging' van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

principe dat je kunt aantonen dat je daadwerkelijk degene bent, die je zegt dat je bent door iets wat je weet en door iets wat je bezit of wat je bent.

1. *Wat je weet* (bijvoorbeeld: wachtwoord / PIN code)
2. *Wat je bezit* (bijvoorbeeld: token, certificaat of via SMS-authenticatie)
3. *Wie je bent* (bijvoorbeeld: biometrisch kenmerk)

Op deze manier kan op basis van twee (ook wel twee factor authenticatie genoemd) of meerdere factoren worden aangetoond dat je daadwerkelijk bent wie je zegt dat je bent. In de 'Gebruiksvoorwaarden voor telewerken' kunnen de voorwaarden voor gebruik van het token worden opgenomen.

## De telewerker zelf

De mens is vaak de zwakste schakel en dat geldt ook bij het telewerken. Zeker wanneer deze zich niet bewust is van de mogelijke risico's die verbonden zijn aan telewerken:

- Het apparaat wordt onbeheerd achtergelaten in een ruimte waar derden toegang tot hebben.
- Men heeft (vaak) niet in de gaten dat men het slachtoffer is van 'social engineering'.<sup>40</sup> Bij social engineering wordt gebruik gemaakt van kwaadwillende personen om van medewerkers informatie te ontfutselen. Dit kan gaan om bedrijfsgeheimen of informatie die niet voor iedereen bestemd is uit gemeentelijke systemen. Denk hier aan bijvoorbeeld wachtwoorden, ontwikkelingsplannen, verblijfplaatsen van mensen. De social engineer maakt gebruik van zwakheden in de mens om zijn doel te bereiken. Meestal is men zich hier niet goed van bewust. Het is heel normaal om een onbekende op de gang aan te spreken en te vragen of ze hulp nodig hebben. Toch hebben veel mensen hier moeite mee en gebeurt het niet. Het is ook goed om je af te vragen met wie je spreekt aan de telefoon en jezelf de vraag te stellen 'waarom wordt me deze vraag gesteld?'.<sup>41</sup>
- Privé-computers thuis worden niet goed beheerd en kunnen besmet raken met malware.<sup>41</sup>

De medewerker moet beveiligingsbewust zijn en weten welke risico's gepaard gaan met telewerken. Dit beveiligingsbewustzijn kan men door middel van een bewustwordingscampagne versterken door gebruik te maken van presentaties of posters over beveiliging.<sup>42</sup> Ook via berichten op de intranetsite van de gemeente, informatiebeveiliging periodiek agenderen tijdens het (afdelings)overleg, opnemen in de planning- en controlcyclus zijn mogelijk om de (informatie)beveiliging onder de aandacht van de medewerkers te brengen. Belangrijk is wel dat dit vanuit een duidelijke visie wordt aangepakt, waarbij een onderbouwing wordt gegeven waarom een bepaalde manier van telewerken noodzakelijk is.

Verder wordt aanbevolen om afspraken te maken over de rechten en plichten van de medewerker, alsook de mogelijke gevolgen bij een geconstateerde overtreding duidelijk te communiceren. De bepalingen kan men in de 'Gebruiksvoorwaarden voor telewerken' opnemen.

Technische beveiligingsmaatregelen helpen tegen ongeautoriseerd gebruik en beschadiging, maar daarnaast zijn gedragsregels nodig voor het omgaan met bedrijfsinformatie in een 'onbeheerde' omgeving buiten de kantoor muren. Denk hierbij aan papieren in de afvalbak en de omgeving die een blik kan werpen op het beeldscherm of kan meeluisteren bij vertrouwelijke gesprekken.

<sup>40</sup> [http://nl.wikipedia.org/wiki/Social\\_engineering\\_%28informatica%29](http://nl.wikipedia.org/wiki/Social_engineering_%28informatica%29)

<sup>41</sup> <http://nl.wikipedia.org/wiki/Malware>

<sup>42</sup> Zie hiervoor ook het operationele product 'Communicatieplan' van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

## **Bijlage 1: Gebruiksvoorwaarden voor telewerken gemeente <naam gemeente>**

Spreek gebruiksvoorwaarden/gedragsregels af rond telewerken. Ter inspiratie is hieronder een aantal mogelijke gebruiksvoorwaarden/gedragsregels beschreven.

1. De telewerker moet zijn privé-apparaat voorzien van een:
  - Up-to-date virusscanner
  - Personal firewall
  - Anti malware tool
  - Screensaver beveiligd met een wachtwoord
  - Up-to-date besturingssysteem en applicaties.
2. Het is de telewerker verboden om bedrijfsinformatie lokaal op het privé-apparaat op te slaan.
3. De telewerker dient als een goede huisvader te zorgen voor de aan hem beschikbaar gestelde apparatuur (zoals apparaat en authenticatie token), en zelf geen applicaties te installeren zonder toestemming van de beheerorganisatie.
4. Er wordt aangegeven op welke locaties de telewerker mag telewerken. Zo kan bijvoorbeeld verboden worden om vanuit een internetcafé of via een onbeveiligde (openbare) draadloze verbinding te telewerken.
5. Er zijn afspraken opgenomen over de rechten en plichten van de medewerker, alsook de mogelijke gevolgen bij een geconstateerde overtreding.

## **Bijlage 2: Telewerk aanwijzing gemeente <naam gemeente>**

### **Uitgangspunten telewerken**

Ten behoeve van het telewerken dienen er regels binnen de gemeente te zijn, die gehanteerd moeten worden als telewerken wordt geïntroduceerd. Het doel van deze aanwijzing is om te voorkomen dat de dienstverlening van de gemeente hinder ondervindt van de risico's in geval van gedeeltelijk of geheel verlies, of beschadiging van data en/of programmatuur en hardware. Er dient binnen de gemeente ook nagedacht te worden over welke diensten wel, en welke diensten zeker niet vanuit de thuiswerkplek of andere apparaten mogen worden geraadpleegd.

De volgende regels dienen terug te komen in het gemeentelijk aanvullend beleid betreffende telewerken, als deze niet al opgenomen zijn in gemeentelijke integriteitsregels:

1. Het opstellen van een telewerkovereenkomst<sup>43</sup>. In deze overeenkomst staan afspraken die betrekking hebben op het telewerken. In deze overeenkomst is aandacht voor:
  - Afspraken tussen verantwoordelijke en telewerker.
  - De duur van de overeenkomst.
  - Telewerkvorm, tijdstippen dat wordt getelewerkt.
  - Taken die op de telewerkplek (mogen) worden uitgevoerd.
  - Afspraken over voortgang, terugkoppeling, bereikbaarheid et cetera.
  - In een aparte bruikleenovereenkomst is aangegeven welke apparatuur door de gemeente is verstrekt, en onder welke condities dit is gebeurd.
  - Aanvullende benodigde (technische) voorzieningen en ondersteuning.
  - In verband met de beveiliging van de informatie moeten onderstaande aanwijzingen door de telewerker worden opgevolgd:
    - Aanwijzingen die betrekking hebben op virusprotectie.
    - Aanwijzingen die betrekking hebben op het beschermen van gevoelige informatie:
      - Plaats geen gevoelige informatie op mobiele apparaten of draagbare opslagmedia zonder versleuteling.
      - Mobiele apparaten worden 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 apparaat wordt ingeleverd, afgedankt of verkocht.
      - Laat de mobiele apparaten niet in een onbeheerd vervoermiddel liggen en vervoer deze niet in het zicht. Bijvoorbeeld op de voorstoel, achterbank of op de vloer.
      - Bescherm mobiele apparaten, indien mogelijk, tegen diefstal door gebruik te maken van een kabelslot/antidiefstalkabel. Met deze kabel kan het mobiele apparaat gekoppeld worden aan een vast object.

<sup>43</sup> Zie ook de databank praktijkvoorbeelden van de Vereniging van Nederlandse Gemeenten (VNG).  
<http://praktijkvoorbeelden.vng.nl/databank/arbeidszaken-en-personeelsbeleid/arbo/telewerken.aspx>

- Aanwijzingen die betrekking hebben op het verzenden en ontvangen van gevoelige informatie.
  - Aanwijzingen die betrekking hebben op het omgaan met wachtwoorden en login-procedures.
  - Aanwijzingen die betrekking hebben op hard- en software:
    - Installeer geen ongeautoriseerde hard- en software.
    - Installeer geen eigen software of download deze niet van een onbekende bron of van het Internet.
    - Gebruik alleen gelicenseerde software.
2. Het opstellen van regels voor acceptabel gebruik. Deze regels dienen door de medewerker geaccepteerd en getekend te worden. Binnen de regels voor acceptabel gebruik is aandacht voor:
- Het proces in geval van verlies of diefstal van alle mobiele apparaten, waarbij meldingen binnen 4 uur gedaan moeten worden.
  - Niet voldoen aan beleid en regels kan resulteren in een disciplinair proces volgens de CAR/UWO<sup>44</sup>.
  - 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.
3. Gebruikers hebben kennis van de regels:
- De risico's met betrekking tot telewerken dienen aandacht te krijgen in bewustwordings- en trainingsmateriaal van de gemeente.
  - Illegale software mag niet worden gebruikt voor de uitvoering van het werk.
4. Toevoegen van regels voor het meenemen van informatie:
- De gemeente dient ook aandacht te hebben voor de impliciete toestemming aan gebruikers welke informatie zij wel of niet mogen inzien tijdens het telewerken, of
  - Er dient duidelijk te worden gemaakt dat de medewerker achteraf ter verantwoording geroepen kan worden.
5. Detailregels om te zorgen voor bescherming van gegevens tijdens het telewerken:
- De gemeente hanteert classificatieregels van gemeentelijke gegevens en zorgt voor passende maatregelen om dit bij telewerken (al of niet) te ondersteunen.
  - Bedrijfsapplicaties worden bij voorkeur zo aangeboden dat er geen gemeentelijke informatie wordt opgeslagen op het apparaat ('zero footprint'). Gemeentelijke informatie en bedrijfsinformatie van derde partijen, waar de gemeente niet de bronhouder van is, maar via het gemeentelijk platform wordt ontsloten dient te worden versleuteld bij transport en opslag, conform classificatie eisen.
- Een alternatief om decentrale opslag van gemeentelijke gegevens te voorkomen is Virtuele Desktop Infrastructuur (VDI). Het stelt wel extra eisen aan de serveromgeving en het netwerk maar voor het beheer betekent de virtuele desktop vaak een efficiencyslag. Door het centrale beheer is het mogelijk om met relatief lage

---

<sup>44</sup> CAR/UWO = Collectieve Arbeidsvoorwaardenregeling en Uitwerkingsovereenkomst voor de sector gemeenten  
<http://www.car-uwv.nl/>

beheerinspanning de medewerker op ieder tijdstip, vanaf iedere willekeurige plek en met ieder willekeurig apparaat in te loggen, veilig, flexibel en gecontroleerd toegang te geven tot zijn persoonlijke werkplek.

- Mocht er toch gemeentelijke informatie of bedrijfsinformatie van derde partijen (waar de gemeente niet de bronhouder van is maar via het gemeentelijk platform wordt ontsloten) op het apparaat worden opgeslagen dan geldt dat er geen plicht bestaat het eigen apparaat te beveiligen, maar de gemeentelijke informatie of die van derden partijen daarop wel.
  - Voorzieningen als webmail, 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.
6. Alle mobiele apparaten, zowel van de gemeente of privé, waarop gemeentelijke informatie of bedrijfsinformatie van derde partijen (waar de gemeente niet de bronhouder van is maar via het gemeentelijk platform wordt ontsloten) kunnen staan, worden bij voorkeur beheerd met een MDM.



## **Bijlage 3: Definities**

**Beveiligingspatroon** Een beveiligingspatroon, als onderdeel van de architectuur is een standaard beschrijving van een probleem en oplossing binnen een bepaalde context, met als doel dat de oplossing algemener inzetbaar wordt. Patronen zijn te beschouwen als bouwstenen op architectuurniveau. Vanuit het perspectief van kennisdeling begint een patroon waar een 'best practice' ophoudt. Waar de Code voor Informatiebeveiliging (ISO 27002) aangeeft dat er een scheiding moet zijn tussen een intern en een extern netwerk, geven patronen aan op welke wijze dit het beste kan gebeuren. Dit is afhankelijk van de specifieke context en in samenhang moet oplossingen bieden die de business nodig heeft.

**Certificaten:** Certificaten zijn gebaseerd op publieke sleuteltechnologie. Hierbij worden twee cryptografische sleutels gegenereerd, een privésleutel en een publieke sleutel. Deze sleutelparen zijn aan elkaar gekoppeld en zijn uniek voor elk individu. De publieke sleutel wordt ondertekend door een Certificate Service Provider (CSP) met als resultaat een X.509-certificaat<sup>45</sup>. De CSP verklaart daarmee, dat deze publieke sleutel toebehoort aan het betreffende individu.

**Hardening:** Hardening is het proces waarbij overbodige functies in besturingssystemen uitgeschakeld worden en/of van het systeem verwijderd worden. En daarnaast door zodanige waarden toekennen aan beveiligingsinstellingen dat hiermee de mogelijkheden om een systeem te compromitteren worden verlaagd en een maximale veiligheid ontstaat. Het gaat hierbij ook om het verwijderen van niet gebruikte of onnodige gebruikers accounts, en tevens het wijzigen van standaard wachtwoorden die op sommige systemen aanwezig kunnen zijn. Met systemen wordt in dit verband bedoeld: servers, actieve netwerkcomponenten zoals Firewalls en switches, desktops, laptops, mobiele apparaten. Kortom, alles met een besturingssysteem. Het resultaat is een gehard systeem.

**Hybride VPN:** Een Hybride VPN is een combinatie van de twee eerder genoemde, waarbij er een secure VPN over een trusted VPN wordt gerealiseerd.

**IP Security (IPSec):** IPSec is een versleutelingmechanisme voor IP-netwerken dat end-to-end beveiliging levert op de netwerklaag (laag 3) van het OSI-model. Het biedt vertrouwelijkheid, integriteit van de data en authenticiteit van de afzender van de data, door het toepassen van verscheidene protocollen en encryptie technieken. IPSec wordt vaak gebruikt in combinatie met een tunneling protocol, zoals L2TP (Layer 2 Tunnel Protocol), om trusted VPN's beter te beveiligen.

**Jailbreak:** Jailbreak is het mogelijk maken van het draaien van niet goedgekeurde apps op een iOS apparaat, waardoor ook malware gedraaid kan worden.

**Man-in-the-middle (MITM):** Een man-in-the-middle-aanval is een aanval waarbij informatie tussen twee communicerende partijen onderschept wordt, zonder dat beide partijen daar weet van hebben. Dit terwijl de computer van de aanvaller zich tussen deze partijen bevindt.

**One-Time Password token:** Met het One-Time Password (OTP) token wordt een wachtwoord van 6 tot 8 cijfers gegenereerd en weergegeven op de display van het persoonsgebonden OTP-token. Met een OTP-token wordt het wachtwoord voor toegang tot een afgeschermd bron continu gewijzigd.

**PINpad token:** Een PINpad Token is voorzien van een display en een toetsenbord om een PIN in te kunnen voeren. Met behulp van dit PINpad Token wordt na invoeren van een PIN code op het token zelf een One-Time Password gegenereerd.

**Rooten:** Rooten is het proces dat het mogelijk maakt men meer rechten krijgt op het apparaat (Android) en daardoor het complete besturingssysteem te wijzigen of te vervangen, en daarmee malware introduceren en gemeentelijke beveiligingsinstellingen te omzeilen.

**Secure Shell (SSH):** Secure Shell (SSH) is ontwikkeld als veilig alternatief voor de onveilige beheerprotocollen zoals telnet, rlogin, rsh en ftp. In tegenstelling tot deze protocollen biedt SSH

<sup>45</sup> <http://www.ietf.org/rfc/rfc2459.txt>

# INFORMATIE BEVEILIGINGS DIENST

versleuteling en 'strong authentication'. Met SSH wordt een beveiligde tunnel opgezet tussen client en server, waardoor het veilig is om gevoelige data, zoals logingegevens, versleuteld te transporteren.

**Secure Sockets Layer (SSL):** Secure Sockets Layer (SSL) en de opvolger hiervan, Transport Layer Security (TLS), zijn protocollen die communicatie over het internet beveiligen. Beide protocollen leveren door middel van versleuteling zowel authenticatie als een beveiligde verbinding over het internet.

**Secure VPN:** Een Secure VPN wordt gerealiseerd door het verkeer tussen twee computers te versleutelen. Hierdoor is het mogelijk om een verbinding via een publieke telecommunicatie infrastructuur, zoals het internet, op te zetten zonder dat de oorspronkelijke data door derden kan worden gelezen. Dit biedt grotendeels de functionaliteit van private huurlijnen tegen veel lagere kosten, door gebruik te maken van de gedeelde publieke, niet vertrouwde infrastructuur.

**Server Based Computing (SBC):** Bij Server Based Computing (SBC) werkt de medewerker in een sessie op de server. Alleen de invoer (muis, toetsenbord) en uitvoer (scherm) worden van/naar het apparaat van de telewerker gestuurd. Dit kan zowel via een SBC client als via een standaard webbrowser.

**SMS-Authenticatie:** Gebruikers die willen inloggen met behulp van SMS Authenticatie vullen naast hun gebruikersnaam en wachtwoord een extra transactiecode in, die de betreffende gebruiker ontvangt per SMS op zijn/haar mobiele telefoon.

**Social engineering:** Bij social engineering wordt gebruik gemaakt van kwaadwillende personen om van medewerkers informatie te ontfutselen. Dit kan gaan om bedrijfsgeheimen of informatie die niet voor iedereen bestemd is uit gemeentelijke systemen. Denk hier aan bijvoorbeeld wachtwoorden, ontwikkelingsplannen, verblijfplaatsen van mensen. De social engineer maakt gebruik van zwakheden in de mens om zijn doel te bereiken. Meestal is men zich hier niet goed van bewust. Het is heel normaal om een onbekende op de gang aan te spreken en te vragen of ze hulp nodig hebben. Toch hebben veel mensen hier moeite mee en gebeurt het niet. Het is ook goed om je af te vragen met wie je spreekt aan de telefoon en jezelf de vraag te stellen 'waarom wordt me deze vraag gesteld'.

**Transport Layer Security (TLS):** Zie Secure Sockets Layer (SSL).

**Trusted VPN:** Een Trusted VPN is opgebouwd uit gehuurde verbindingen die via het netwerk van een netwerk- of internet provider lopen. Exclusiviteit staat of valt bij de belofte van de provider dat niemand anders gebruik maakt van dezelfde verbinding. Hierdoor kunnen eigen IP-adressering en beveiligingsprocedures worden gebruikt. De klant vertrouwt erop dat de provider de integriteit van de verbinding bewaakt, vandaar trusted.

**Virtuele Desktop Infrastructuur (VDI):** Deze infrastructuur laat toe om op afstand (bijvoorbeeld via het internet) en met een eigen apparaat, te werken op een virtueel besturingssysteem dat niet op het lokale apparaat, maar op de server draait. Om met een virtuele desktop te werken, moet een VDI-client op het apparaat geïnstalleerd zijn die de verbinding maakt met het virtuele besturingssysteem op de server.

**Virtueel Particulier Netwerk (VPN):** Een Virtual Private Network (VPN) is een privé datanetwerk, dat gebruik maakt van een publieke telecommunicatie infrastructuur. Privacy wordt hierbij gerealiseerd door gebruik te maken van een tunneling-protocol en beveiligingsprocedures. Men onderscheidt drie vormen van VPN's, te weten trusted VPN's, secure VPN's en hybride VPN's.

## **Bijlage 4: Literatuur/bronnen**

Voor deze publicatie is gebruik gemaakt van onderstaande bronnen:

**Titel: Whitepaper Telewerken**

Wie: Nationaal Cyber Security Centrum (NCSC)

Datum: 04 februari 2009

Link: <https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/telewerken.html>

**Titel: Beveiliging van Telewerken: een praktische aanpak**

Wie: NOREA - de beroepsorganisatie van IT-auditors in Nederland

Wat: Tijdschrift De EDP-Auditor / IT-Auditor 2/2011

Datum: 2011

Link: [http://www.norea.nl/Norea/Actueel/Recente+publicaties/Tijdschrift+De+EDP-Auditor/IT\\_Auditor\\_2\\_2011.aspx?item=2](http://www.norea.nl/Norea/Actueel/Recente+publicaties/Tijdschrift+De+EDP-Auditor/IT_Auditor_2_2011.aspx?item=2)

# INFORMATIE BEVEILIGINGS DIENST

|

**INFORMATIEBEVEILIGINGSDIENST  
VOOR GEMEENTEN (IBD)**

**NASSAULAAN 12  
2514 JS DEN HAAG**

**POSTBUS 30435  
2500 GK DEN HAAG**

**HELPDESK 070 373 80 11  
ALGEMEEN 070 373 80 08  
FAX 070 363 56 82**

**[IBD@KINGGEMEENTEN.NL](mailto:IBD@KINGGEMEENTEN.NL)  
[WWW.KINGGEMEENTEN.NL](http://WWW.KINGGEMEENTEN.NL)**



KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN  
VERENIGING VAN NEDERLANDSE GEMEENTEN