



## Microdata Services – Remote Access Maatregelenbeleid

	Omschrijving	Maatregel <sup>1</sup>
<b>Geringe overtreding</b>	<p>Als een actie van de Remote Access (RA) gebruiker leidt tot een incident dan is er sprake van een geringe overtreding. Een <b>incident</b> is een gebeurtenis of omstandigheid die processen van het CBS kan verstoren.</p> <p>Als incident wordt in ieder geval beschouwd:</p> <ol style="list-style-type: none"> <li>1. Het niet melden van de vermissing, verlies of diefstal van:               <ol style="list-style-type: none"> <li>a. een RA gebruikersnaam en/of wachtwoord;</li> <li>b. een bij het CBS aangemelde telefoon voor de RA SMS code;</li> <li>c. een door het CBS verstrekt RA token;</li> </ol> </li> <li>2. Het uitlenen of onveilig bewaren van de onder 1 a t/m c genoemde zaken; of</li> <li>3. Het zonder akkoord van het CBS met onbevoegden delen van informatie uit door het CBS gecontroleerde output op het moment dat deze output nog niet openbaar gepubliceerd is.</li> </ol>	<p>Waarschuwingsbrief aan de leidinggevende van de onderzoeker(s) én de betrokken onderzoeker(s) moet(en) (opnieuw) een awarenesstest met goed gevolg afleggen alvorens weer toegang te krijgen tot RA. De overtreding wordt 3 jaar vastgelegd. Als er binnen 3 jaar na het eerste incident een nieuw incident wordt gemeld binnen een project of bij dezelfde onderzoeker, dan wordt die overtreding minimaal beschouwd als een ernstige overtreding.</p>
<b>Ernstige overtreding</b>	<p>Als een actie van de Remote Access (RA) gebruiker leidt tot een beveiligingsincident dan is er sprake van een ernstige overtreding. Een <b>beveiligingsincident</b> is een incident waarbij <b>mogelijk</b> de vertrouwelijkheid, integriteit of beschikbaarheid van binnen het CBS beschikbare gegevens is geschonden.</p> <p>Als ernstige overtreding wordt in ieder geval beschouwd:</p> <ol style="list-style-type: none"> <li>1. Het omzeilen van de outputcontrole door RA <i>geaggregeerde</i> gegevens van het beeldscherm over te schrijven, te fotograferen, etc.;</li> <li>2. Werken in een openbare ruimte;</li> <li>3. Werken op een computer waarmee de Remote Access omgeving wordt benaderd via een openbaar wifi netwerk (bijvoorbeeld in de trein, het café, etc.);</li> <li>4. Een onbevoegde persoon in de RA omgeving laten werken;</li> <li>5. Op andere wijze de vertrouwelijkheid van de CBS gegevens schenden:</li> </ol>	<p>Waarschuwingsbrief aan de leidinggevende van de onderzoeker(s) en/of intrekken van de inlogrechten van de betrokken onderzoeker(s) voor de periode van maximaal 6 maanden, afhankelijk van de ernst van de overtreding en de intensiteit van het gebruik van RA voorzieningen. De betrokken onderzoeker(s) moet(en) (opnieuw) een awarenesstest met goed gevolg afleggen alvorens weer toegang te krijgen tot RA. De organisatie van de onderzoeker(s) dient maatregelen te treffen om herhaling te voorkomen. De overtreding wordt 3 jaar vastgelegd. Indien er binnen 3 jaar een nieuw incident wordt gemeld binnen een project of bij dezelfde onderzoeker, dan</p>

<sup>1</sup> Tegen dit besluit kan degene wiens belang rechtstreeks daarbij is betrokken binnen 6 weken na de dag van verzending van de maatregelbrief een gemotiveerd bezwaarschrift indienen bij de Directeur-Generaal van de Statistiek, p/a Centraal Bureau voor de Statistiek, Postbus 24500, 2490 HA Den Haag.

Welke maatregel wordt toegepast en wat de duur daarvan is, wordt aan de hand van de belastende bewijzen bepaald door de directeur Statistische Dienstverlening en Informatieverstrekking (SDI) en het hoofd Microdata Services.

	<p>6. Een geringe overtreding, indien er in de 3 jaar voorafgaand aan dit incident reeds een geringe overtreding heeft plaatsgevonden binnen hetzelfde project of bij dezelfde onderzoeker; of</p> <p>7. Een situatie waarbij meerdere geringe overtredingen plaatsvinden.</p>	<p>wordt die overtreding beschouwd als een zeer ernstige overtreding.</p>
<p><b>Zeern ernstige overtreding</b></p>	<p>Als een actie van de Remote Access (RA) gebruiker leidt tot een datalek dan is er sprake van een zeer ernstige overtreding. Een <b>datalek</b> is een beveiligingsincident waarbij <i>persoons- of bedrijfsgegevens</i> verloren zijn gegaan of waarbij redelijkerwijs niet kan worden uitgesloten dat persoons- of bedrijfsgegevens onrechtmatig zijn verwerkt (zie voor volledige definitie de website van de Autoriteit Persoonsgegevens).</p> <p>Als zeer ernstige overtreding wordt in ieder geval beschouwd:</p> <ol style="list-style-type: none"> <li>1. Het omzeilen van de outputcontrole door RA <i>persoons- of bedrijfsgegevens</i> van het beeldscherm over te schrijven, te fotograferen, etc.;</li> <li>2. Het op een ander wijze veroorzaken van een datalek of daaraan bijdragen;</li> <li>3. Een ernstige overtreding indien er in de 3 jaar voorafgaand aan dit incident reeds een ernstige overtreding heeft plaatsgevonden binnen hetzelfde project of bij dezelfde onderzoeker; of</li> <li>4. Een situatie waarbij meerdere ernstige overtredingen plaatsvinden.</li> </ol>	<p>Opschorten van de projectovereenkomst met <u>alle</u> betrokken onderzoekers voor een periode van minimaal 6 maanden, afhankelijk van de ernst van de overtreding en de intensiteit van het gebruik van RA voorzieningen. Alle tokens van betrokken onderzoekers worden gedurende de maatregelperiode gedeactiveerd. De betrokken onderzoekers moeten (opnieuw) een awarenessstest met goed gevolg afleggen alvorens weer toegang te krijgen tot RA. De organisatie van de onderzoekers dient maatregelen te treffen om herhaling te voorkomen. Na de maatregelperiode kan de organisatie een verzoek voor herstart van het project bij CBS indienen. Of de projectovereenkomst door CBS wordt voortgezet, is mede afhankelijk van de maatregelen die de organisatie treft om herhaling te voorkomen. Afhankelijk van de ernst van de overtreding kunnen ook algemene maatregelen genomen worden tegen de contractpartij en/of de instelling waarvoor de betrokken onderzoekers werkzaam zijn. In het uiterste geval kan dit resulteren in intrekking van de instellingsmachtiging. De overtreding wordt 3 jaar vastgelegd.</p>