Microdata Services – Remote Access Sanctioning Policy
Version January 2022

	Description	Sanction[1]
Minor breach	If an action by the Remote Access (RA) user leads to an incident, this is a minor breach. An ***incident*** is a disturbing event or circumstance that may cause disruption of Statistics Netherlands' (hereinafter CBS) processes. The following is considered an incident in any case: 1. Failure to report the missing, loss or theft of: a. RA username and/or password; b. a phone that has been registered with CBS for the RA SMS code; c. RA token provided by CBS; 2. Lending or unsafe storage of the items referred to under 1 a to c; or 3. Sharing information from CBS-controlled outputs with unauthorized persons without the consent of CBS if this output has not been published publicly.	Warning letter to the supervisor of the researcher(s) and the researcher(s) involved must (again) pass an awareness test before being allowed access to RA again. The breach shall be recorded for 3 years. If a new incident is reported within 3 years after the first incident within the same project or involving the same researcher, then that breach is considered a severe breach at least.
Severe breach	If an action by the Remote Access (RA) user leads to a security incident, this is a severe breach. A ***security incident*** is an incident which **possibly** violates the confidentiality, integrity or availability of data available within CBS. The following breaches are considered severe in any case: 1. Bypassing the output control by copying, photographing etc. of RA *aggregated* data from the monitor; 2. Working in a public space; 3. Working on a computer which connects to the Remote Access via a public WiFi network (for example on trains, in cafes etc.); 4. Letting an unauthorised person work in the RA environment; 5. Otherwise violating the confidentiality of the data provided;	Warning letter to the supervisor of the researcher(s) and/or revocation of login rights of the researcher(s) involved for a period of up to 6 months, depending on the seriousness of the breach and the intensity of the use of RA facilities. The researcher(s) involved must (again) pass an awareness test before being allowed access to RA again. The organisation of the researcher(s) must take measures to prevent recurrence. The breach shall be recorded for 3 years. If a new incident is reported within 3 years after the first incident within the same project or involving the same researcher, then that breach is considered a very severe breach.

[1] This decision can be appealed against by the person who is directly affected by the decision. Any appeal must motivated and be submitted within six weeks from the date of dispatch of the sanction letter. The appeal can be sent to: The Director General of Statistics, c/o Statistics Netherlands, PO Box 24500, 2490 HA The Hague, the Netherlands.
The type of sanction and its duration will be determined on the basis of the incriminating evidence by the director of SDI (Statistical Services and Information) and the head of Microdata Services.

	6. A minor breach if a minor breach has already taken place within the same project or involving the same researcher in the 3 years prior to the incident; or 7. A situation in which several minor breaches occur.	
Very severe breach	If an action by the Remote Access (RA) user leads to a data breach, then there is a very severe breach. A ***data breach*** is a security incident in which *personal or business data* have been lost or in which it cannot reasonably be ruled out that personal or business data were processed unlawfully (a full definition can be found on the website of the Dutch Data Protection Authority (Autoriteit Persoonsgegevens). The following breaches are considered very severe in any case: 1. Bypassing the output control by copying, photographing etc. of RA *personal or business data* from the monitor; 2. Otherwise causing or contributing to a data breach; 3. A severe breach if a severe breach has already taken place within the same project or involving the same researcher in the 3 years prior to the incident; or 4. A situation in which several severe breaches occur.	Suspension of the project agreement for <u>all</u> researchers involved for a period of at least 6 months, depending on the seriousness of the breach and the intensity of the use of RA facilities. All tokens of researchers involved are deactivated during the suspension period. The researchers involved must (again) pass an awareness test before being allowed access to RA again. The organisation of the researcher(s) must take measures to prevent recurrence. After the suspension period, the organisation may submit a request with CBS for restarting the project. Whether the project agreement is continued by CBS also depends on the measures taken by the organisation to prevent recurrence. Depending on the seriousness of the violation, general measures may also be taken against the contractor and/or the institution employing the researchers involved. In very serious cases this can lead to the revoking of the institution's authorization. The breach shall be recorded for 3 years.