Basisafspraken Informatiebeveiliging voor Onderzoeksopdrachten Ministerie van Onderwijs, Cultuur en Wetenschap (OCW)

1. Inleiding

1.1 Dit document bevat de minimale informatiebeveiligingsvereisten die gelden voor onderzoeksbureaus die in opdracht van het Ministerie van OCW werken. Op basis van een risicoafweging per onderzoeksopdracht kunnen voorafgaand aan de opdrachtuitvoering aanvullende beveiligingsmaatregelen worden bepaald die passend zijn bij de bijzondere aard van de onderzochte informatie of de te onderzoeken doelgroep en gevoeligheid van het onderzoek.

---

2. Algemene Beveiligingseisen

2.1 De opdrachtnemer dient te voldoen aan maatregelen uit de Baseline Informatiebeveiliging Overheid (BIO) of maatregelen die hieraan gelijk zijn gesteld, en aan relevante wet- en regelgeving.

2.2 Onderzoeksdata dient in overleg met opdrachtgever conform de BIO te worden geclassificeerd en beschermd.

---

3. Technische Beveiligingsmaatregelen

3.1. De opdrachtnemer dient passende technische beveiligingsmaatregelen op alle betrokken devices, netwerk- en servercomponenten te implementeren, waaronder:

- Versleuteling van onderzoeksgegevens bij opslag en transport.
- Toegangsbeheer met sterke multi-factor authenticatie.
- Functiescheiding op basis van ‘need to know’.
- Logging en monitoring van toegang tot onderzoeksdata.
- Tijdige implementatie van beveiligingsupdates en patches.

---

4. Organisatorische Beveiligingsmaatregelen

4.1 Medewerkers die toegang hebben tot onderzoeksdata dienen een geheimhoudingsverklaring (NDA) te ondertekenen en/of in het bezit te zijn van een recent Verklaring Omtrent Gedrag (VOG).

4.2 Er dienen duidelijke richtlijnen en gedragsregels te zijn voor het gebruik van privé-apparaten (BYOD) en thuiswerken.

4.3 De opdrachtnemer dient een exit-strategie te hebben voor veilige overdracht of vernietiging van onderzoeksdata bij beëindiging van de overeenkomst.

---

5. Compliance en Verantwoording

5.1 De opdrachtnemer dient jaarlijks een in control verklaring (ICV) of certificering (bijv. ISO 27001 of een Third Party Memorandum) te overleggen over de informatiebeveiliging*.
5.2 Beveiligingsincidenten met mogelijke impact op onderzoeksdata dienen direct te worden gemeld aan OCW en de opdrachtnemer dient medewerking te verlenen bij onderzoek naar de oorzaak en gevolgen.
5.3 OCW behoudt het recht om audits uit te voeren op de informatiebeveiliging van de opdrachtnemer en diens ketenpartners.

---

6. Aanvullende Maatregelen op Basis van Risicoanalyse

6.1 Opdrachten met een verhoogd risicoprofiel kunnen aanvullende beveiligingseisen met zich meebrengen, zoals:

- Strengere toegangscontroles.
- Specifieke eisen ten aanzien van datalokalisatie en cloudgebruik.
- Extra eisen rondom beveiliging van fysieke opslagmedia.
- Extra eisen rondom toegang en gedrag.

---

7. Sancties en Beëindiging

7.1 Niet-naleving van deze afspraken kan leiden tot ingebrekestelling of verzuim en uiteindelijk tot opschorting of beëindiging van de opdracht.
7.2 Eventuele schade als gevolg van niet-nakoming van deze eisen kan worden verhaald op de opdrachtnemer.

---

8. Slotbepalingen

8.1 Dit document vormt de basis voor informatiebeveiliging bij alle onderzoeksopdrachten en wordt als bijlage toegevoegd aan iedere opdrachtovereenkomst.
8.2 Indien wijzigingen in wet- en regelgeving dit noodzakelijk maken, kunnen de eisen in dit document worden herzien.

* Bureaus die niet gecertificeerd zijn kunnen een In Control Verklaring (ICV) overleggen. Een voorbeeld van zo'n ICV is als achtergrondinformatie toegevoegd bij de aanbestedingsdocumenten.