Statuut voor informatiebeveiliging / Information Security Policy

Country Manager
March 2026
versie 2.1

Inleiding

Ipsos I&O is een onderzoeksbureau voor markt- en beleidsonderzoek. De grondstof van Ipsos I&O is data. En dit vraagt dat we op een zorgvuldige manier met data omgaan. Niet alleen om de wettelijk eisen (waaronder de AVG, Auteurswet en Telecommunicatiewet) na te leven maar ook om de reputatie en daarmee de continuïteit van Ipsos I&O te waarborgen.

We hebben een Quality and Information Security Management System (QIMS) volgens de norm ISO27001, ISO9001, ISO20252 en ISO27701. Hierin hebben we vastgelegd hoe we gezamenlijk omgaan met informatie van ons bedrijf en van onze klanten. Ipsos I&O wil een hoog beveiligingsniveau kunnen garanderen zodat onze klanten hun informatie met een gerust hart aan ons toevertrouwen. Dit statuut vormt het beleidskader voor de betrouwbaarheid en beschikbaarheid van de informatievoorziening bij Ipsos I&O. Binnen dit kader is een evenwichtig (kosten - baten) stelsel van maatregelen ontwikkeld met als doel onze informatiesystemen te beschermen tegen interne en externe bedreigingen.

Opzet

Van elk informatiesysteem is één houder benoemd. Het houderschap impliceert de eindverantwoordelijkheid voor het betreffende systeem, inclusief risico's, beveiliging en interne controlemaatregelen. Naast de applicatie betreft dit ook de infrastructurele componenten (werkstations, servers en netwerken), beheer, het maken van afspraken met derden, fysieke beveiliging en het managen van calamiteiten. Er wordt gesproken over eindverantwoordelijk, omdat een aantal aspecten van het informatiesysteem uitbesteed wordt aan andere houders.

De maatregelen en de prioriteitsstelling hierin, worden bepaald op grond van een periodiek op te stellen risicoanalyse. Deze risicoanalyse omvat het signaleren van bedreigingen die samenhangen met de informatievoorziening en het ontwikkelen van hierbij aansluitende maatregelen. Hierbij wordt niet een maximaal beveiligingsniveau nagestreefd, maar een optimaal niveau voor Ipsos I&O.

Beleidsuitgangspunten

Beleidsuitgangspunt vormen de doelstellingen van de norm NEN-ISO/IEC 27001:2022 voor zover zij bijdragen aan de informatiebeveiliging en NEN-ISO/IEC 27701:2019 voor privacy.

Bij het vaststellen van het informatiebeveiligingsbeleid in dit statuut is geborgd dat:

- het beleid passend is voor Ipsos I&O;
- er op basis van dit beleid doelstellingen zijn geformuleerd;
- er een verbintenis is om te voldoen aan de QIMS eisen en het proces van continu verbeteren;
- het beleid gedocumenteerd en bekend is binnen de organisatie en daar waar relevant bij overige belanghebbenden.

Beleidsdoelstellingen
Ons informatiebeveiligingsbeleid heeft de volgende doelstellingen:

1. Bescherming van de vertrouwelijkheid, integriteit en beschikbaarheid van onderzoeksdata en persoonsgegevens;
2. Vermindering van het risico op datalekken en cyberaanvallen;
3. Voldoening aan relevante wet- en regelgeving;
4. Toewijzing van workloads aan de meest geschikte leveranciers (waaronder cloud diensten) op basis van security-eisen.

Specific principles with regard to control measures
Om de informatiebeveiliging in onze organisatie te garanderen, hebben we verschillende maatregelen genomen die voortkomen uit specifieke controls of annexes uit ISO 27001 en die aansluiten bij het beleid van Ipsos Global.

Subject	Policy statement	Relevant documents
Mobile devices / BYOD (A.5.10)	IPSOS I&O, through client contractual obligations, is mandated to store project related data on IPSOS I&O owned and/or controlled services, servers, computers, mobile and tablet devices. As a consequence, IPSOS I&O does not carry a Bring Your Own Device (BYOD) policy for its employees. All mobile devices are allowed, provided the device has up-to-date patches, anti-malware and file encryption.	IPSOS Global Book of Policies and Procedures, section 7: Information and Technology **7.2 Information Security Policy**
Remote working (A.6.7)	Remote work is allowed with approved equipment and secure connections (VPN)	IPSOS Global Book of Policies and Procedures, section 7: Information and Technology **7.2 Information Security Policy**
Access security (A.5.15)	Access security through multi-factor authentication based on best effort and according to the Need to know principle for information classified as confidential and higher.	IPSOS Global Book of Policies and Procedures, section 7: Information and Technology **7.2 Information Security Policy** **7.4. Information classification chapter 4**
Cryptographic controls (A.5.12 and A.8.24)	Transport, message and data encryption based on classification.	IPSOS Global Book of Policies and Procedures, section 7: Information and Technology

		7.4 Information Management
Clear desk and clear screen policies (A.7.7)	Clear screen & Clear desk policy applies to confidential and secret information, for both physical and IT workplaces.	IPSOS Global Book of Policies and Procedures, section 7: Information and Technology **7.2 Information Security Policy**
Data backup (A.8.13)	Backups are performed redundantly based on classification, retention (also) outside the physical location with 28 days of retention and a corresponding test schedule (check)	IPSOS Global Book of Policies and Procedures, section 7: Information and Technology **7.4 Information Management**
Screening (A.6.1)	We want to have every staff member screened.	
Operational software auditing (A.5.10 and A.8.19)	Installation of approved software may be performed by a local admin (check)	IPSOS Global Book of Policies and Procedures, section 7: Information and Technology **7.2 Information Security Policy**
Transmission of information (A.5.14)	Transport, message and data encryption via approved information transport devices based on classification	IPSOS Global Book of Policies and Procedures,section 7: Information and Technology **7.2 Information Security Policy**
Cloud services (A.5.23)	In line with our policy and procedure regarding supplier management, we purchase cloud products (SaaS, IaaS, BaaS, etc.) based on purchasing requirements regarding information security, among other things. We also periodically assess whether such suppliers provide services in accordance with our information security requirements.	

Eindverantwoordelijkheid
Gelet op de mogelijke impact van verstoringen op de continuïteit van Ipsos I&O, berust de eindverantwoordelijkheid voor het beleid inzake informatiebeveiliging bij de Country Manager van Ipsos I&O.

Leiderschap
Bij het werken aan en concretiseren van de beleidsuitgangspunten heeft de directie van Ipsos I&O zelf een actieve rol en is zij maximaal betrokken.

De directieverantwoordelijkheden hierbij betreffen:

- het bewerkstelligen dat het informatiebeveiligings- en privacybeleid en de bijbehorende doelstellingen zijn vastgesteld en maximaal aansluiten bij de strategie van Ipsos I&O;
- het bewerkstelligen dat de eisen van het QIMS in de bedrijfsvoering van Ipsos I&O is geïntegreerd;
- het bewerkstelligen dat de voor het QIMS benodigde middelen beschikbaar zijn;
- het belang van een effectief QIMS en het voldoen aan de eisen communiceren;
- het bewerkstelligen dat het QIMS de beoogde resultaten behaalt;
- het aansturen van de medewerkers en deze ook te ondersteunen om een bijdrage te leveren aan het QIMS;
- het bevorderen van het proces van continu verbeteren;
- het ondersteunen van managementfuncties om hun leiderschap te tonen binnen hun verantwoordelijkheidsgebieden.

Rol personeel

Het personeelsbeleid van Ipsos I&O is mede gericht op het leveren van een bijdrage aan de vertrouwelijkheid, integriteit en continuïteit van de informatievoorziening en de privacy. Wanneer het voor de uitoefening van de werkzaamheden noodzakelijk is, is het personeel bevoegd om bedrijfsmiddelen buiten de kantoorlocaties van Ipsos I&O te gebruiken. Het personeel mag mobiele apparatuur zoals laptops alsmede documenten zoals ingevulde vragenlijsten niet onbeheerd achterlaten. Leiderschap op het gebied van informatiebeveiliging betekent dat we alert zijn, waar mogelijk het goede voorbeeld geven, elkaar helpen en aanspreken op ongewenst gedrag. Hierbij heeft het management een voorbeeldfunctie, maar ook van medewerkers wordt een proactieve houding verwacht. Op hoofdlijnen gelden hierbij de volgende verantwoordelijkheden, die verder zijn uitgewerkt in de procedures die verband houden met informatiebeveiliging, zoals vastgelegd in ons Kwaliteitshandboek QIMS.

Alle functies:
- Nemen kennis van het beleid zoals gepubliceerd in het Kwaliteitshandboek QIMS en de (gedocumenteerde) beheersmaatregelen en passen dit toe;
- Spreken elkaar aan op ongewenst gedrag, melden incidenten en houden zich aan het datalekprotocol;
- Volgen instructies met betrekking tot informatiebeveiliging, in de ruimste zin van het woord op;
- Nemen actief deel aan awareness campagnes, trainingen en instructies.

Security officer:
- Bewaakt dat het QIMS aan ISO 27001/ISO 27701 voldoet;
- Organiseert audits en voorziet in rapportages;
- Identificeert eisen uit o.a. wetgeving, contracten en certificeringsnormen;
- Adviseert en ondersteunt bij het bewaken van vervaldata, risico analyses, dataclassificatie, oorzaakanalyses, calamiteitenoefeningen en systeemevaluaties;

Bijzondere ICT rollen (administrator):
- Passen principes voor secure architecture en secure development toe;
- Delen kennis over informatiebeveiliging binnen het team;
- Signaleren en melden afwijkingen in systemen pro-actief.

Leidinggevenden (lead):
- Signaleren risico's/nemen deel aan risico analyses en implementeren beheersmaatregelen;
- Vervullen een voortrekkersrol bij het verbeteren van bewustzijn;
- Meten, analyseren en sturen bij op basis van KPI, audits en incidentmeldingen;
- Verbeteren maatregelen op grond van risico(her)beoordelingen en oorzaakanalyses.

De organisatie maakt voor specialistische kennis en ondersteuning gebruik van een extern adviesbureau. Voor de overige medewerkers zijn de verantwoordelijkheden en bevoegdheden verwoord in het informatiebeveiligingsbeleid en de procedures die tot het Kwaliteitshandboek QIMS behoren.

Bovenstaande en overige beleidsregels inzake informatiebeveiliging worden, ook bij wijzigingen, aan medewerkers medegedeeld. Naleving van deze regels wordt door de directie verplicht gesteld.

Werkzaamheden derden
Het uitvoeren van werkzaamheden door leveranciers worden zodanig omgeven met maatregelen (waaronder verwerkersovereenkomsten), dat er geen inbreuk op de vertrouwelijkheid, integriteit en continuïteit van de informatievoorziening en privacy kan ontstaan.

Privacy
Bij de verwerking en het gebruik van gegevens worden maatregelen getroffen om de privacy van klanten, respondenten en personeel te waarborgen, ook op het gebied van bijzondere persoonsgegevens zoals gezondheidsinformatie.

Toegang informatie
Toegangsbeveiliging zorgt ervoor dat ongeautoriseerde personen of processen geen toegang krijgen tot de geautomatiseerde systemen, gegevensbestanden en programmatuur van Ipsos I&O.

Opslag gegevens
Het beheer en de opslag van gegevens zijn zodanig, dat geen informatie verloren kan gaan.

Gegevensverstrekking
Gegevensverstrekking intern en extern gebeurt op basis van 'need to know'. Medewerkers treffen maatregelen om te voorkomen dat informatie in handen van personen terechtkomt, die deze informatie niet strikt nodig hebben. Het Kwaliteitshandboek QIMS met bijbehorende procesbeschrijvingen en trainingen geeft hiervoor de benodigde handvatten. Ook de toegang tot informatiesystemen wordt volgens het principe van 'need to know' adequaat beveiligd. Voor ICT-medewerkers wordt hierop een uitzondering gemaakt, om te komen tot een betere service aan de gebruikers.

Datatransport
Datatransport is zodanig met beveiligingsmaatregelen omkleed, dat geen inbreuk kan worden gepleegd op de vertrouwelijkheid en de integriteit van de gegevens. We stellen een beveiligde up- en downloadserver beschikbaar voor het uitwisselen van bestanden met persoonsgegevens. Deze en andere instructies ten aanzien van het niet onbeheerd achterlaten van laptops, het vergrendelen van de computer, clear desk beleid en andere concrete maatregelen waar medewerkers zich aan houden staan in de Informatiefolder Informatiebeveiliging bij Ipsos I&O die nieuwe medewerkers krijgen uitgereikt bij hun arbeidscontract.

Programmatuur licenties
Teneinde computervirusinfecties te voorkomen wordt er slechts gewerkt met geautoriseerde versies van (legale) programmatuur.

Inrichting informatiesystemen
Alle verantwoordelijke medewerkers dienen bij te dragen aan de inrichting van de organisatie, procedures, werkwijze en de daarbij gehanteerde informatiesystemen. Dit statuut vormt hiervoor het kader.

Beveiliging
De fysieke en logistieke beveiliging van de kantoorlocaties van Ipsos I&O is zodanig, dat de vertrouwelijkheid, integriteit en beschikbaarheid van de gegevens en gegevensverwerking gewaarborgd zijn.

Veranderingen
Aanschaf, installatie en onderhoud van gegevensverwerkende systemen, alsmede inpassing van nieuwe technologieën, mogen geen afbreuk doen aan het niveau van veiligheid van de totale informatievoorziening.

Afhandeling incidenten
Er is een proces om incidenten adequaat af te handelen en hier 'lessons learned' uit te trekken. De Medewerkersfolder Basisregels voor Informatiebeveiliging (ook in het Engels beschikbaar) bij Ipsos I&O die nieuwe medewerkers krijgen uitgereikt bij hun arbeidscontract bevat instructies ten aanzien van het melden van incidenten.

Continuïteit bedrijfsvoering
Er zijn calamiteitenplannen en -voorzieningen om de continuïteit van de bedrijfsvoering en de informatievoorziening te waarborgen en imagoschade te voorkomen.

Gewijzigd vastgesteld door drs. B.G. Huijgen
9-3-2026
Country Manager van Ipsos I&O.