Informatie-beveiligingsbeleid

Populytics BV
Versie: 1.0
Goedgekeurd door management: 4 maart 2025
Classificatie: Openbaar

1 Context en doelen

Wij van Populytics geloven dat de wereld beter wordt wanneer beleid goed aansluit bij de waarden, voorkeuren en overtuigingen van de mensen waar het over gaat. Daarom maken we raadplegingen die een grote en diverse groep mensen bereiken. Hiermee stellen we politici, bestuurders en beleidsmakers in staat doeltreffend beleid te maken.

Dit beleidsdocument beschrijft het informatiebeveiligingsmanagementsysteem (ISMS) dat onze organisatie gebruikt. Iedereen in onze organisatie (of op sleutelposities bij leveranciers) die vertrouwelijke of gevoelige gegevens verwerkt, moet op de hoogte zijn van dit beleid en handelen in overeenstemming met het beleid. Ook als iemand iets in ons bedrijf waarneemt dat niet in overeenstemming is met dit beleid, moet hij of zij dit onmiddellijk melden. Dit kan worden gedaan door het beveiligingsteam op de hoogte te stellen via infosec@populytics.nl. Het volledige managementteam van ons bedrijf is betrokken geweest bij het opstellen van dit beleid en zet zich volledig in om ervoor te zorgen dat we ons aan de regels houden.

Wij formuleren periodiek doelen, monitoren de voortgang en sturen bij waar nodig.

2 Scope

De scope van het ISMS is:
Informatiebeveiliging gerelateerd aan het ontwerpen en aanbieden van online raadplegingen en onderzoeken, en de analyse en rapportage van de resultaten daarvan, en alle werkzaamheden die nodig zijn om dit te realiseren.

In deze scope bieden wij de volgende hoofdactiviteiten en diensten aan klanten:

- Ontwerpen van raadplegingen en onderzoeken in ons eigen platform Wevaluate
- Toegang bieden tot platform Wevaluate voor het ontwikkelen en uitvoeren van raadpleging en/of onderzoek
- Verzamelen van data als onderdeel van de raadpleging en/of onderzoek
- Analyseren en rapporteren van de resultaten van raadplegingen en/of onderzoeken

Op dit moment zijn er geen afdelingen of bedrijfsactiviteiten specifiek buiten de scope van dit beleid verklaard. Ons bedrijf heeft de volgende kantoorlocaties en werklocaties die binnen het bereik van dit beleid vallen:

- Kantoor: Strawinskylaan 339, 1077XX Amsterdam

Populytics BV managet haar datacentrum niet direct. Amazon Web Services wordt gebruikt als leverancier van de IT-infrastructuur.

3 Stakeholder analyse

Het managementteam is verantwoordelijk voor het onderhouden van regelmatig contact met belanghebbenden, het begrijpen van de informatiebeveiligingseisen en verwachtingen van belanghebbenden en ervoor te zorgen dat het ISMS hierop is afgestemd. De resulterende informatie is gedocumenteerd in de stakeholderanalyse, die jaarlijks zal worden bijgewerkt.

4 Leiderschap

Het gehele management is op de hoogte van het informatiebeveiligingsbeleid en is vastbesloten om deze inspanning op permanente basis te ondersteunen. Shira Hollanders is de managementvertegenwoordiger die rechtstreeks in contact staat met het beveiligingsteam.

Er is een informatiebeveiligingsteam (INFOSEC-team) dat verantwoordelijk is voor het implementeren en onderhouden van informatiebeveiliging. De verantwoordelijkheden van het informatiebeveiligingsteam en andere rollen zijn vastgelegd.

Alle personeelsleden van de organisatie worden regelmatig ingelicht door het informatiebeveiligingsteam en zijn verantwoordelijk voor het volgen van het beleid en de richtlijnen.

5 Middelen, awareness en training

Het management is ervoor verantwoordelijk dat werknemers die informatiebeveiligingstaken uitvoeren uitgebreide kennis hebben van de onderwerpen waaraan zij werken. Ze krijgen een security awareness training na het afsluiten van het contract en daarna weer minstens één keer per jaar. Medewerkers die betrokken zijn bij het ontwerpen en ontwikkelen van producten of personeel met extra beveiligingsverantwoordelijkheden zullen extra training krijgen die geschikt is voor hun rol.

6 Planning

Het INFOSEC-team en management stelt doelen en KPI’s vast om de effectiviteit van het ISMS te meten. Het INFOSEC-team voert de metingen uit en zorgt dat meetresultaten worden besproken. Er is een jaarplanning waarin terugkerende overleggen en acties zijn vastgelegd.

7 Prestatie evaluatie

Het managementteam zal de effectiviteit van het ISMS jaarlijks beoordelen in een management review. Indien nodig zal ondersteuning door externe partners worden gezocht, zoals aanvullend technisch advies, onafhankelijke beveiligingstests of audits door onafhankelijke partijen.

8 Continue verbetering

Het management is gecommitteerd om het ISMS continu te verbeteren. Dit wordt gedaan door belanghebbenden te documenteren en te analyseren en externe bronnen van expertise te raadplegen.