Beleid beveiliging en privacy

Document	Beleid beveiliging en privacy
Auteur(s)	Susan Gussinklo
Datum	Mei 2022
Versie	1.1

Versie	Datum	Auteur	Opmerking
1.0	1-1-2022	SG	Start document
1.1	Mei 2022	Directie	Vaststellen

1. Doel beveiliging

In dit document beschrijven we hoe DataCare en haar applicaties informatie verwerken en beschermen. Er wordt verwezen naar andere documenten. Samen vormt dit het beleid waarin richtlijnen rondom gegevensbescherming worden vastgelegd. We specificeren welke maatregelen we nemen om veiligheid te garanderen en hoe we omgaan met incidenten. Afspraken en richtlijnen rondom informatiebeveiliging worden vastgelegd, zodat duidelijk is aan welke richtlijnen moet worden voldaan.

We bieden iedere klant een verwerkersovereenkomst aan. DataCare zorgt ervoor dat de gegevens van haar (interne) klanten goed worden beschermd. Klanten maken gebruik van de applicaties van DataCare middels een Microsoft of een Google Account. De verantwoordelijkheid van deze accounts ligt bij de klant. Alle documenten die betrekking hebben op ons privacybeleid zijn op aanvraag in te zien.

In dit document *1-Beleid beveiliging en privacy* beschrijven we hoe DataCare omgaat met de beveiliging en privacy van gegevens. Minimaal 1x per jaar lopen we het beleid en de bijbehorende documenten na en updaten we deze waar nodig. Bijbehorende documenten:

2- overzicht uitbestede processen DataCare
3- beheer bedrijfsmiddelen-software-documenten
4- procedure toegangsbeveiliging en autorisatie
5- procedure incidentenbeheer en datalek, incidentenregistratie
6- procedure beheer van Documenten
7- verwerkersovereenkomst

2. Organisatie en verantwoordelijkheden

- Directie is eindverantwoordelijk.
- Ownership wordt vastgesteld voor elk kritisch informatiesysteem. De eigenaar bepaalt hoe beveiligingsmaatregelen worden gebruikt en beheerd in overeenstemming met het beveiligingsbeleid.
- Systeembeheerder/Ontwikkelaars, raadplegen, coördineren en controleren status van de beveiliging en geven voorstellen voor aanpassingen op richtlijnen en procedures. Ontwikkelaars kunnen op verzoek van klant in de database kijken om zo een vraag te beantwoorden of een bug op te sporen. Gegevens worden nooit voor andere doeleinden gebruikt.
- Een supportmedewerker kan op verzoek van een klant bij een supportmelding de database raadplegen. De medewerker is zich ervan bewust dat in de productieomgeving van de klant gekeken/gewerkt wordt. Gegevens worden nooit voor andere doeleinden gebruikt.
- Alle werknemers zijn verantwoordelijk voor het naleven van het beveiligingsbeleid en worden hierover geïnformeerd middels werkoverleggen / check-in / personeelsdocument en gecontroleerd en aangesproken middels collega's en directie.

3. Communicatie

Het beleid van DataCare wordt via de website www.edumaps.nl gecommuniceerd.