Informatiebeveiligingsbeleid eLoo

(Conform ISO/IEC 27001:2022)
Versie 1.0 (nov 2026)

1. Doel en beleidsverklaring

eLoo ontwikkelt en beheert software voor kwaliteitsmonitoring in het onderwijs en verwerkt daarbij informatie van klanten, gebruikers, medewerkers en andere stakeholders. Informatiebeveiliging is essentieel voor het waarborgen van vertrouwen, continuïteit en compliance.

De directie van eLoo committeert zich expliciet aan:

- Het beschermen van de vertrouwelijkheid, integriteit en beschikbaarheid van informatie en -systemen;
- Het naleven van wet- en regelgeving, waaronder de Algemene Verordening Gegevensbescherming (AVG), zoals nader toegelicht in de privacyverklaring van eLoo;
- Het voldoen aan contractuele verplichtingen en verwachtingen van stakeholders;
- Het implementeren, onderhouden en continu verbeteren van een Information Security Management System (ISMS) volgens NEN-EN-ISO/IEC 27001:2022 per 1-1-2027;
- Het beschikbaar stellen van voldoende middelen, capaciteit en bevoegdheden voor informatiebeveiliging.

Dit informatiebeveiligingsbeleid vormt het overkoepelende kader voor het vaststellen van informatiebeveiliging doelstellingen en voor het beheersen van informatiebeveiligingsrisico's binnen eLoo.

2. Beveiligingsprincipes

eLoo hanteert de volgende kernprincipes voor informatiebeveiliging:

- **Risicogebaseerde aanpak**
  Beveiligingsmaatregelen worden vastgesteld op basis van risicoanalyse.
- **Least privilege**
  Toegang tot informatie en systemen wordt beperkt tot wat noodzakelijk is voor iemands functie.
- **Need-to-know**
  Informatie wordt uitsluitend gedeeld indien dit noodzakelijk is voor het doel.
- **Secure by design & secure by default**
  Beveiliging is geïntegreerd in het ontwerp, de ontwikkeling en het beheer van systemen en diensten. AI-functionaliteit wordt alleen in producten en diensten toegepast na een vooraf goedgekeurde risicobeoordeling.

- **Defence in depth**
  Meervoudige, elkaar aanvullende beveiligingsmaatregelen worden toegepast.
- **Continu verbeteren (PDCA)**
  Informatiebeveiliging wordt periodiek geëvalueerd en waar nodig verbeterd.
- **Verantwoord gebruik van AI**
  AI-toepassingen worden alleen ingezet als ze zijn goedgekeurd en als de risico's vooraf zijn beoordeeld. Vertrouwelijke informatie en persoonsgegevens worden alleen verwerkt in AI-toepassingen die daarvoor zijn goedgekeurd en die voldoen aan de AVG. Dit gebeurt conform het AI-beleid van TSS.

3. Informatiebeveiligingsdoelstellingen

eLoo stelt meetbare informatiebeveiligingsdoelstellingen vast, waaronder:

- Beschikbaarheid van systemen volgens SLA-afspraken;
- Tijdige detectie en afhandeling van informatiebeveiligingsincidenten;
- Periodieke uitvoering en actualisatie van risicoanalyses;
- Aantoonbare compliance met interne en externe audits.

De voortgang wordt gemonitord via KPI's en periodiek geëvalueerd.

4. ISMS en procesbenadering (PDCA)

Het ISMS is ingericht volgens de Plan – Do – Check – Act - cyclus:

- **Plan** – beleid, risicoanalyse en doelstellingen vaststellen;
- **Do** – implementeren van beheersmaatregelen;
- **Check** – monitoring, audits en metingen uitvoeren;
- **Act** – bijsturen en verbeteren.

Het ISMS is geïntegreerd in de primaire processen:

- Research & Development (R&D)
- Sales & Marketing (S&M)
- Professional Services (PS)
- Customer Support (CS)
- General & Administration (G&A)

5. Beheersmaatregelen en beleidshiërarchie

- **TSS Code of Conduct (2026)**
  Van toepassing op eLoo als onderdeel van de TSS-groep. Bevat onder andere richtlijnen over integriteit, bescherming van persoonsgegevens, verantwoordelijk IT-gebruik en het melden van incidenten.

- **Personeelsregels Informatiebeveiliging eLoo**
  Bevatten operationele gedragsregels voor medewerkers, waaronder aanvaardbaar gebruik van bedrijfsmiddelen, wachtwoordgebruik, clean desk & clear screen, werken op afstand en het melden van beveiligingsincidenten.
- **TSS Security Control Framework (SCF)**
  Groepsbreed framework van de TSS-groep, waaraan alle business units moeten voldoen, dus ook eLoo. Het SCF bevat de concrete beheersmaatregelen waarmee eLoo dit beleid in de praktijk uitvoert. Het SCF omvat tien gebieden: beheer van bedrijfsmiddelen, gegevensbescherming en naleving van de AVG, technische kwetsbaarheden, toegangsbeheer, bescherming tegen dataverlies, detectie van inbreuken, beveiliging van producten en diensten, security awareness, voorbereiding op calamiteiten en het melden van beveiligingsincidenten. Het SCF geldt voor eLoo zelf en voor leveranciers die namens eLoo IT-systemen beheren of gegevens verwerken. Zij rapporteren hier periodiek over.
- **Privacyverklaring eLoo**
  Publiek beschikbare verklaring waarin wordt toegelicht hoe eLoo persoonsgegevens verwerkt, beveiligt en de rechten van betrokkenen waarborgt conform de AVG: https://eloo.nl/privacyverklaring-eloo/

Samen vormen deze documenten een samenhangend stelsel van beleid, gedragsregels, beheersmaatregelen en transparantie richting medewerkers, klanten en overige stakeholders. Bij tegenstrijdigheden prevaleert dit informatiebeveiligingsbeleid, tenzij wettelijke of groepsbrede regelgeving anders bepaalt.

6. Bewustwording en naleving

eLoo bevordert informatiebeveiligingsbewustzijn door:

- Training en awareness-programma's, waaronder over verantwoord gebruik van AI;
- Interne communicatie;
- Richtlijnen en procedures;
- Kennisname en naleving van de Huisregels Informatiebeveiliging en de TSS Code of Conduct.

Naleving van dit beleid is verplicht voor alle medewerkers en relevante externe partijen.

7. Monitoring, auditing en verbetering

De effectiviteit van het ISMS wordt beoordeeld via:

- Interne en externe audits;
- Managementreviews en KPI-monitoring;
- Periodieke rapportages en self-assessments op basis van het TSS Security Control Framework;
- Incident- en trendanalyses.

Verbetermaatregelen worden vastgelegd, opgevolgd en geëvalueerd.

8. Review en onderhoud van het beleid

Dit informatiebeveiligingsbeleid wordt:

- Minimaal jaarlijks beoordeeld;
- Herzien bij significante wijzigingen in de organisatie, wetgeving, dreigingen of technologie.

Wijzigingen worden formeel goedgekeurd door de directie.

9. Slotverklaring

Dit informatiebeveiligingsbeleid is van toepassing op alle medewerkers, systemen en processen binnen de scope van het ISMS en wordt actief uitgedragen binnen de organisatie.
Op verzoek kan dit beleid beschikbaar worden gesteld aan relevante stakeholders.

Datum: 1 november 2026
Directie eLoo