Klik Onderwijs

Informatiebeveiligingsbeleid

Versie: 1.3 - september 2022

1 Inleiding

Het succes van Klik onderwijs en haar klanten is in hoge mate afhankelijk van de door Klik Onderwijs zelf ontwikkelde applicaties en computer platforms. In onze platforms en applicaties ligt informatie opgeslagen de van belang is voor een adequate bedrijfsvoering van onze klanten en onszelf. Omdat de digitale wereld steeds aan verandering onderhevig is brengt dat ook mogelijke bedreigingen risico's met zich mee. Het is daarom vanzelfsprekend dat KLIK Onderwijs zorgdraagt voor een adequate informatiebeveiliging en daarmee voldoet aan relevante wet- en regelgeving.

Informatiebeveiliging is een beleidsverantwoordelijkheid van de directie van Klik Onderwijs. Informatiebeveiliging is niet een éénmalige actie. Door wijzigingen in de organisatie en daarbuiten wordt bij Klik Onderwijs continu aandacht besteedt aan informatiebeveiliging.

2 Doelstelling

Het informatiebeveiligingsbeleid heeft als doel bij te dragen aan de kwaliteit van de informatievoorziening voor haar klanten en zichzelf en zorgdragen voor een optimale balans tussen functionaliteit, veiligheid, privacy en kosten.

3 Toepassingsgebied en scope

Toepassingsgebied

Klik Onderwijs is een onderwijsdienstverlener die scholen en stichtingen helpt om de kwaliteit van hun onderwijs en organisatie te versterken. Dit zodat zij optimaal invulling kunnen geven aan wat leerlingen, hun ouders, en de samenleving van hen vraagt. Klik Onderwijs ondersteunt hen met advies, training en performance support en met het Klik Platform. Het eerste integrale digitale platform dat dankzij de unieke leerdoelenstructuur daadwerkelijk zicht en grip geeft op het leerproces van de leerling en de relevante werkprocessen in de school; 24 uur per dag, zeven dagen per week. Dit stelt elke school, ongeacht het soort onderwijs, in staat om grip te houden en daar waar nodig bij te sturen. En deze grip vereenvoudigt de verantwoording naar de onderwijsinspectie.

Wij bieden de volgende diensten aan klanten:

- Software-platform;
- Training & performance support;
- Advies.

Hierbij zijn de volgende teams en afdelingen betrokken:

1. Team Markt dat weer is onderverdeeld naar Team Marketing & Sales, Team Relatie en Accountmanagement en Team Propositie.
2. Team ProductServices.
3. Team Curriculum & Expertise.

4. Team Infrastructuur.
5. Staf: Finance, HR en Media & Communicatie.

Scope

Klik Onderwijs hanteert de scope voor haar informatiebeveilingsbeleid:

Het beveiligen van informatie in relatie tot het ontwikkelen en leveren van een modulair IT onderwijsplatform en leerlingvolgsysteem, inclusief customer support, ten behoeve van het funderend onderwijs.

Op dit moment zijn er geen afdelingen of bedrijfsactiviteiten specifiek buiten de scope van dit beleid verklaard.

Klik Onderwijs heeft geen eigen datacentrum. Alle data is gehost bij betrouwbare cloudproviders.

4 Beleidsprincipes en -uitgangspunten

Beleidsprincipes

Klik Onderwijs hanteert de volgende principes in haar informatiebeveilingsbeleid:

1. **Risicogebaseerd**
   We baseren de maatregelen op de mogelijke veiligheidsrisico's van onze informatie, processen en IT-faciliteiten.

2. **Iedereen**
   Iedereen is en voelt zich verantwoordelijk voor een juist en veilig gebruik van middelen en bevoegdheden.

3. **Lijnverantwoordelijkheid**
   De directie is overall verantwoordelijk voor de informatiebeveiliging. Leidinggevenden drage de verantwoordelijkheid voor de informatiebeveiliging binnen hun afdeling.

4. **Secure by Design**
   Informatiebeveiliging is vanaf de start een integraal onderdeel van ieder project of iedere verandering m.b.t. informatie, processen en IT-faciliteiten.

5. **Secure by Default**
   Gebruikers hebben alleen toegang tot informatie en IT-faciliteiten die zij nodig hebben voor hun werkzaamheden. Het openstellen van informatie is een bewuste keuze.

6. **Continu verbeterproces**
   Op periodieke wijze worden beleid en maatregelen getoetst.

Uitgangspunten

Uit de doelstelling van informatiebeveiliging vloeien de volgende uitgangspunten voort:

- **Kader**
  Het beleid biedt een kader om (toekomstige) maatregelen in de informatiebeveiliging te toetsen aan de bovengenoemde beveiligingsprincipes (hoofdstuk 4), best practices en normen. Daarnaast biedt het een kader om de taken, bevoegdheden en verantwoordelijkheden in de instelling te beleggen.

- **Normen**
  Klik Onderwijs baseert de normen voor informatiebeveiliging op ISO 27001. ISO 27001 is met dit informatiebeveiligingsbeleid de basis voor een informatiebeveiligingsmanagementsysteem (ISMS). Het ISMS is ingericht op basis van de internationale standaard ISO 27001. Formele certificering volgens de norm ISO 27001 ziet Klik Onderwijs als noodzakelijk.

- **Maatregelen**
  Klik Onderwijs treft maatregelen op basis van de internationaal vastgestelde ISO-27001 standaard.

- **Communicatie**
  Communicatie over informatiebeveiliging wordt actief bevorderd.

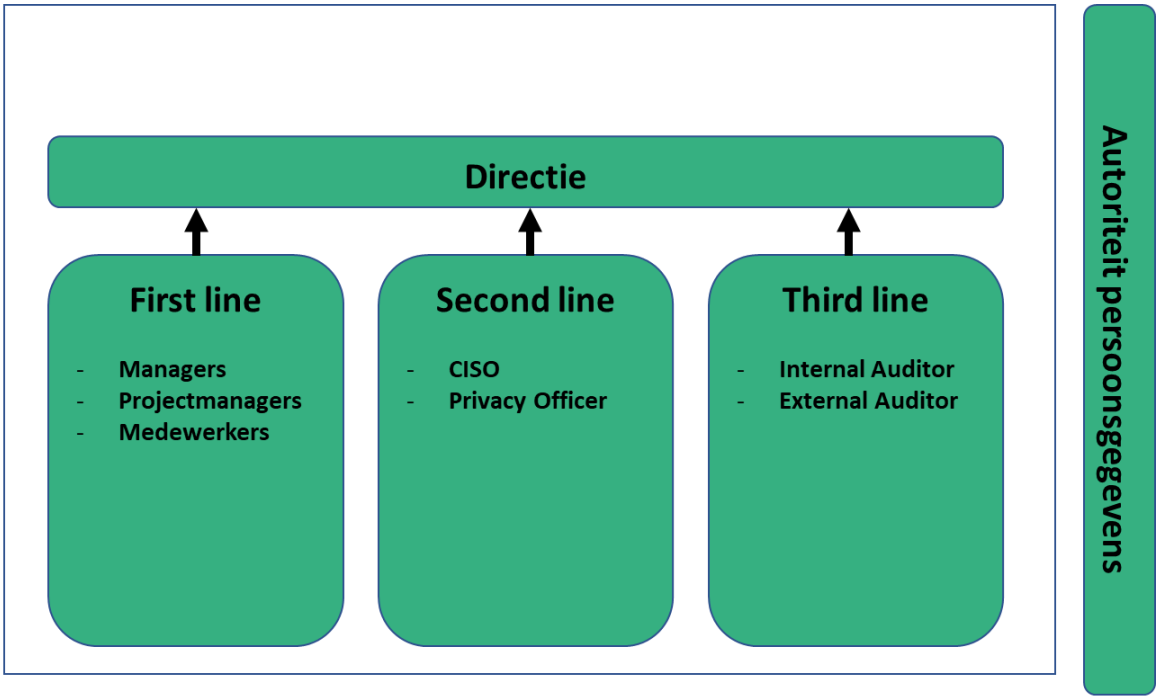
5 Wet- en regelgeving

Uitgangspunt is dat Klik Onderwijs voldoet aan alle van toepassing zijnde wet- en regelgeving en zich voorbereidt om aan opkomende wetgeving tijdig te voldoen. (zie voor meer details het handboek Informatiebeveiliging A18)

6 Governance

Organisatie van de beveiligingsfunctie

De organisatie van de beveiligingsfunctie is opgebouwd volgens het 3-lines of defense model. (zie voor meer details het handboek Informatiebeveiliging A6 en A8)



Schema: Three Lines of Defense

Directie

De directie is eindverantwoordelijk voor de informatiebeveiliging binnen Klik Onderwijs en stelt het beleid en de basismaatregelen op het gebied van informatiebeveiliging vast. De portefeuillehouder van de informatiebeveiliging bij Klik Onderwijs is belegd bij de COO. De COO is tevens verantwoordelijk voor de professionalisering van de informatiebeveiliging.

First line

Informatieveiligheid begint bij de leidinggevenden en de medewerkers. Dit houdt in dat zij eindverantwoordelijk zijn eigen informatiebeveiliging binnen de eigen invloedssfeer.. Leidinggevenden en medewerkers dienen de door Klik Onderwijs voorgeschreven beveiligingsmiddelen en informatiebeveiligingsmaatregelen te gebruiken en te volgen. Zij zijn zich bewust van relevante wet- en regelgeving en signaleren (potentiële) beveiligingsincidenten.

De 1st line is tevens verantwoordelijk voor de invoering van beheersmaatregelen en aanleveren van bewijsmateriaal dat aan de normen wordt voldaan.

Second line

De CISO rapporteert direct aan de COO. De CISO draagt zorg voor de toepassing en naleving van het informatiebeveiligingsbeleid en bewaakt de compliance ten aanzien van relevante wet- en regelgeving, adviseert over informatiebeveiligingsmaatregelen en bewaakt de consistentie van de maatregelen. Daarnaast is BCM (Business Continuity Management) belegd bij CISO functie alsmede de rol van Privacy Officer (PO).

De 2nd line is tevens verantwoordelijk voor het opstellen van het Informatiebeveiligingsbeleid, het opstellen van het privacy beleid, de normen en het toetsen van de naleving van de normen/beheersmaatregelen op dit gebied.

Third line

Internal and external audit zijn verantwoordelijk voor het toetsen van het beleid en als onafhankelijke partij.

Bewustwording en training

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van informatiebeveiliging uit te sluiten. De mens zelf creëert de grootste risico's. Bij Klik Onderwijs werken we daarom voortdurend aan het verhogen van het beveiligingsbewustzijn van medewerkers met als doel om kennis van risico's te verbeteren en veilig en verantwoord gedrag aan te moedigen. Onderdeel van het beleid zijn regelmatig terugkerende bewustwordingscampagnes voor alle medewerkers en derden en met name operationele beheerders en ontwikkelaars.

Overleg

Om de samenhang in de organisatie van de informatiebeveiligingsfunctie goed tot uitdrukking te laten komen en de initiatieven en activiteiten op het gebied van informatiebeveiliging binnen de verschillende onderdelen op elkaar af te stemmen wordt bij gestructureerd overleg gevoerd over het onderwerp informatiebeveiliging op diverse niveaus.

Documenten

Voor informatiebeveiliging wordt bij dezelfde (PDCA-)managementcyclus gevolgd, die ook voor andere onderwerpen geldt: visie/idee, beleid, analyse, plan implementatie, uitvoering, controles en evaluatie. Die cyclus wordt op de verschillende niveaus ondersteund door een aantal formeel vastgestelde documenten.

Daarnaast is aandacht besteed aan:
Bij het opstellen van het informatiebeveiligingsbeleid hebben wij, conform onze Verklaring van Toepasselijkheid, onder meer aandacht besteed aan beleid en maatregelen voor:

- mobiele apparatuur (A.6.2.1);
- disciplinaire procedure m.b.t. datalek (A7.2.3);
- (logische) toegangsbeveiliging (A.9.1.1);
- cryptografie (A.10.1.1);

- clear desk / clear screen (A.11.2.9);
- backup (A.12.3.1);
- informatietransport (A.13.2.1);
- beveiligd ontwikkelen (A.14.2.1);
- leveranciers (A.15.1.1);
- incidentmanagement (A16).

7 Melding en afhandeling van incidenten

Een incident is een gebeurtenis die de bedrijfsvoering negatief kan beïnvloeden. Incidentbeheer en - registratie gaat over het detecteren, vastleggen en afhandelen van incidenten. Belangrijk hierbij is dat medewerkers en derden herkennen wanneer er sprake is van een incident of inbreuk op de informatiebeveiliging en dit ook melden. Van incidenten kan worden geleerd. Incidentregistratie en periodieke rapportage over opgetreden incidenten horen dan ook thuis in een volwassen informatiebeveiligingsomgeving. (zie voor meer details het Handboek informatiebeveiliging A16)

Goedgekeurd door directie: 13-01-2023

Raymond van Kerkvoorden (CEO)