# Informatiebeveiligingsbeleid

## Context en doelen

Deze pagina beschrijft de hoofdlijnen van het informatiebeveiligingsmanagement-systeem (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.
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.

## Scope

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:

- Het Klik Software-platform
- Training & performance support
- Advies

De scope van het ISMS is: Het beveiligen van informatie gerelateerd aan het ontwikkelen en leveren van een modulair IT onderwijsplatform en leerlingvolgsysteem en het geven van ondersteuning en training 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 cloud providers.

## Stakeholderanalyse, beleid en maatregelen

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

# Informatiebeveiligingsbeleid

In ons informatiebeveiligingsbeleid hebben wij, conform onze Verklaring van Toepassing, onder meer aandacht besteed aan beleid en maatregelen voor:

- mobiele apparatuur (A.6.2.1);
- (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).

## Leiderschap

Het gehele management is op de hoogte van het informatiebeveiligingsbeleid en is vastbesloten om deze inspanning op permanente basis te ondersteunen. De Algemeen Directeur is de managementvertegenwoordiger die rechtstreeks in contact staat met het Information Security Team (InfoSec Team). Er is een InfoSec Team dat verantwoordelijk is voor het implementeren en onderhouden van informatiebeveiliging.
Alle andere personeelsleden van het bedrijf worden regelmatig ingelicht door het InfoSec Team en zijn verantwoordelijk voor het volgen van het beleid en de richtlijnen.

## Middelen, awareness en training

De algemeen directeur 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.

## Operations

Het InfoSec Team en het management zijn verantwoordelijk voor het implementeren en onderhouden van de procedures en controles die nodig zijn op basis van regelmatig risicobeoordeling. Het InfoSec Team en het management stellen 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.

## 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.

# Informatiebeveiligingsbeleid

## Continue verbetering

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

Goedgekeurd door directie: 20-5-2022

*Voor meer informatie over informatiebeveiliging bij Klik Onderwijs of voor het doorgeven van geconstateerde verbetermogelijkheden in onze beveiliging, mail naar info@klikonderwijs.nl*