Kennisnet

Beleid voor informatiebeveiliging, privacy en bedrijfscontinuïteit

Versie 1.8

23 mei 2024

Laat ict werken **voor het onderwijs**

Voorwoord

Digitalisering in de maatschappij leidt tot toenemende beschikbaarheid van data en potentieel dus tot nieuwe of rijkere informatie. Dit biedt mogelijkheden om snellere en beter geïnformeerde keuzes te maken. Overal is een app voor – iedereen is online. Zakelijke en publieke diensten bedienen de consument op elk moment van de dag met producten en informatie.

Digitalisering speelt ook een grote rol binnen het onderwijs. Datasturing en informatisering maken het mogelijk om persoonlijk onderwijs te geven en leerlingen op “op maat” lesmateriaal en feedback aan te bieden. Iets dat in een klas van 25 kinderen zonder de inzet van ict praktisch onmogelijk is voor de docent. Tevens raken het onderwijsproces en het bedrijfsvoering proces hierdoor steeds meer met elkaar vervlochten.

Digitalisering brengt ook risico’s met zich mee. Het leidt tot vraagstukken rondom het verzamelen van data en de verschillende vormen van classificatie daarbinnen. Denk daarbij in het bijzonder aan persoonsgegevens. Met welk doel worden ze verzameld, wie beslist hierover, wie heeft ervoor getekend? En indien je met de juiste doelbinding beschikt over data hoe ga je er dan qua beveiliging mee om, zodat je voorkomt dat ze in verkeerde handen kunnen vallen? En omgekeerd: hoe zorg je dat data die wél toegankelijk moet zijn ook altijd beschikbaar is?

Kennisnet ondersteunt het onderwijs in de zorg voor informatiebeveiliging en privacy. Omdat we daarbij zelf het goede voorbeeld willen geven moet informatiebeveiliging en privacy voor de Kennisdiensten en organisatie natuurlijk ook op orde zijn. Daarbij zien we dat de diensten die Kennisnet levert steeds meer verweven zijn in het primaire onderwijsproces. Dit betekent dat we de continuïteit van deze dienstverlening zo goed mogelijk willen waarborgen, ook in het geval van calamiteiten. In dit document laten wij zien aan iedereen met wie wij samenwerken, intern en extern, hoe wij dat georganiseerd hebben.

Voor Kennisnet zijn Informatiebeveiliging, privacy en bedrijfscontinuïteit onlosmakelijk met elkaar verbonden en integraal onderdeel van beleid, processen en uitvoering. We hebben gekozen voor ISO 27001 en ISO 22301 als verzameling van beveiligings- en continuïteitsmaatregelen om ons doorlopend proces van risicoafweging en mitigerende maatregelen vorm te geven. Verder geldt *het by design principe* binnen Kennisnet voor alle dienstverlening, zowel voor security, privacy als bedrijfscontinuïteit. Dit zorgt er ook voor dat het beleid geen papieren tijger is of wordt maar een onderdeel van onze dagelijkse werkwijze.

Marianne Mulder
Directeur Operations

Inhoud

1. Het belang van informatiebeveiliging, privacy en bedrijfscontinuïteit

Informatie en ict zijn de kernactiviteiten van Kennisnet. We leveren diensten aan-, en verwerken informatie van-, een groot aantal belanghebbenden in het onderwijs, waaronder besturen, scholen, raden, ketenpartijen, leerlingen en hun ouders. Hierbij hebben we te maken met een groot aantal mogelijke bedreigingen. Alle systemen die we gebruiken en gegevens die we bewaren en verwerken, kunnen worden bedreigd door bijvoorbeeld een aanval, een vergissing of de natuur (zoals een overstroming of brand).

Datalekken, incorrecte gegevens of diensten die niet beschikbaar zijn – in het ergste geval schaden deze incidenten onze dienstverlening en daarmee het vertrouwen in Kennisnet. Daarom zijn de continuïteit van onze dienstverlening en privacybescherming van groot belang. Ook treffen we gericht maatregelen om mogelijke risico's tot een aanvaardbaar niveau te reduceren.

De directie doet daarom een beroep op iedereen die betrokken is bij de activiteiten van Kennisnet, vanuit een gemeenschappelijke visie en wil, de verwerking van (persoons)gegevens correct te laten verlopen.

Dit beleid gaat dieper in op de bescherming van ict en in het bijzonder persoonsgegevens. Het dient als norm en leidraad voor alle informatieverwerking en biedt een uitgangspunt voor audit en controle.

Dit beleid biedt elke belanghebbende – medewerker, klant of leverancier – een inzage in de manier waarop we omgaan met (persoons)gegevens.

1.1. Scope

Het beleid voor informatiebeveiliging, privacy en continuïteit is van toepassing op de hele organisatie:

- Alle informatieverwerking die plaatsvindt binnen en namens Kennisnet
- Alle diensten die worden geleverd en de diensten die worden ingekocht
- Onze eigen medewerkers, tijdelijk personeel en op personeel dat door derden wordt ingezet om diensten te verlenen aan of namens onze organisatie.
- De middelen die hierbij worden ingezet.

1.2. Doel

Het beleid voor informatiebeveiligings-, privacy- en continuïteit binnen Kennisnet heeft de volgende doelen:

- Het waarborgen van de continuïteit van de dienstverlening van Kennisnet.
- Het beschermen van de privacy van eenieder van wie Kennisnet persoonsgegevens verwerkt.
- Het voorkomen en zo goed mogelijk afhandelen van incidenten.
- Het minimaliseren van de eventuele gevolgen van incidenten.

Bij het realiseren van deze doelen bewaakt Kennisnet de balans tussen werkbaarheid – in de meest brede zin van het woord – en informatiebeveiliging, privacy en bedrijfscontinuïteit.

2. Het beleid

Het beleid bestaat uit keuzes die Kennisnet maakt om de doelen rond informatiebeveiliging, privacy en bedrijfscontinuïteit te bereiken.

2.1. Voorbeeldrol

Kennisnet heeft een voorbeeldrol in de onderwijsketen en communiceert helder en actief over informatiebeveiliging en privacy. Alle medewerkers en diensten van Kennisnet dienen voorbeeldig te zijn wat betreft informatiebeveiliging en privacy.

2.2. Wet- en regelgeving

Kennisnet houdt zich aan alle relevante wet- en regelgeving. Twee regels vormen daarbij de basis:

- De bestuurder van Kennisnet is eindverantwoordelijk voor de bescherming van persoonsgegevens.
- Kennisnet hanteert passende technische en organisatorische maatregelen voor het beschermen van diensten en in het bijzonder persoonsgegevens.

2.3. Betrouwbaarheid

Scholen zijn in toenemende mate afhankelijk van Kennisnet diensten voor het vervullen van hun primaire taak: het geven van goed onderwijs. Dit brengt verantwoordelijkheid met zich mee. Kennisnet treft de nodige maatregelen om bij een storing of een calamiteit de impact op het primaire onderwijsproces te minimaliseren.

2.4. Overal in verweven

Kennisnet beschouwt informatiebeveiliging, privacy en bedrijfscontinuïteit als onlosmakelijk met elkaar verbonden en als belangrijk onderdeel van het beleid, de processen en de uitvoering van diensten. Daar waar mogelijk wordt informatiebeveiliging, privacy en bedrijfscontinuïteit opgenomen in bestaande processen.

2.5. Verantwoordelijkheid van iedereen

Omdat iedereen binnen en rondom Kennisnet bijdraagt aan informatiebeveiliging en privacy, zijn de rollen en verantwoordelijkheden rondom informatiebeveiliging en privacy duidelijk vastgelegd.

2.6. ISO als basis

Kennisnet kiest ISO 27001 als een verzameling van geschikte beveiligingsmaatregelen. Deze norm sluit naadloos aan op ISO 22301, die wordt gebruikt als vertrekpunt om onze bedrijfscontinuïteit te organiseren. De processen voor informatiebeveiliging en continuïteit zijn doorlopend en cyclisch. Dat betekent dat Kennisnet jaarlijks de organisatie als geheel evalueert, controleert en verbetert. Nieuwe ontwikkelingen of incidenten, binnen en buiten Kennisnet, aanschaf van diensten of bedrijfsmiddelen en grote wijzigingen in de dienstverlening zijn aanleiding tot extra valuatie, controle en eventuele bijstelling.

Kennisnet past privacy *by design*, security *by design* en privacy *by default* toe om passende maatregelen te kunnen treffen.

3. Uitvoering

Voor realisatie van het beleid voor informatiebeveiliging, privacy en bedrijfscontinuïteit besteedt Kennisnet aandacht aan een aantal zaken.

3.1. Bewustzijn

Het bevorderen van bewustzijn rondom informatiebeveiliging, privacy en bedrijfscontinuïteit is de verantwoordelijkheid van alle medewerkers. Het beveiligingsbewustzijn wordt vergroot door:

- Voorlichting (security awareness training)
- Opstellen en uitdragen van gedragsregels (handleiding aanvaardbaar gebruik bedrijfsmiddelen)

Deze middelen dragen het volgende uit:

- Het belang van informatiebeveiliging, privacy en bedrijfscontinuïteit voor Kennisnet
- Nieuwe ontwikkelingen op het gebied van informatiebeveiliging en privacy (bijvoorbeeld actuele incidenten)
- De belangrijkste veiligheidsmaatregelen rond dagelijkse werkzaamheden
- Waar mensen terecht kunnen bij incidenten, kwetsbaarheden of met ideeën en vragen

3.2. Kwetsbaarheden, incidenten en datalekken

Medewerkers of andere betrokkenen die een kwetsbaarheid, incident of inbreuk rond informatiebeveiliging en/of privacy zien of vermoeden, dienen dit te melden. Een vraag of suggestie over informatiebeveiliging en privacy kan ook gemeld worden. Alle meldingen worden volgens een vast proces behandeld. Wanneer het om persoonsgegevens gaat, wordt de Functionaris voor de Gegevensbescherming (FG) ingeschakeld. Na afhandeling van het incident wordt de melder ingelicht over de afhandeling daarvan.

Een melding van incidenten of verzoeken rondom persoonsgegevens kan gedaan worden bij de Servicedesk, of via email naar support@kennisnet.nl. In de standaard gebruiksvoorwaarden en disclaimer van Kennisnetdiensten, staat deze loketfunctie vermeld. Externe partijen kunnen bij dit loket ook terecht voor:

- Algemene informatie over de verwerking van persoonsgegevens.
- Verzoeken voor inzage van de eigen verwerkte gegevens en eventuele wijziging of verwijdering daarvan.

3.3. Naleving

Schending van de wetgeving, voorschriften of regels rond informatiebeveiliging en privacy kan leiden tot corrigerende maatregelen zoals non-actiefstelling, disciplinaire straffen en beëindiging van een contract of dienstverband.

3.4. Actualiteit

Kennisnet houdt rekening met actuele ontwikkelingen. Daarom wordt dit beleid minimaal elk jaar getoetst en zo nodig aangepast en opnieuw vastgesteld door het managementteam (MT) aan de hand van het volgende:

- De behoeften en verwachtingen van belanghebbenden in de onderwijsketen
- De status van de informatiebeveiliging als geheel (beleid, organisatie, risico's)
- De effectiviteit van de genomen maatregelen en aantoonbare werking daarvan
- Wet- en regelgeving

3.5. Wet- en regelgeving

Door het aanstellen van een FG en een jurist bewaakt Kennisnet dat we voldoen aan alle relevante wet- en regelgeving. Deze professionals scholen zich op regelmatige basis bij, vertalen de juridische kaders vertalen naar praktische toepassingen en informeren de organisatie hierover. Jaarlijks vindt er een beoordeling plaats, waarbij de relevante wet- en regelgeving in verband met IBP wordt gecontroleerd. Dat geldt onder andere voor:

- De Algemene Verordening Gegevensbescherming en de Uitvoeringswet Algemene verordening gegevensbescherming
- Het Convenant digitale onderwijsmiddelen en Privacy
- De Telecommunicatiewet (spamverbod en cookies)
- Bewaartermijnen in verschillende wet- en regelgeving (belastingwetten, archiefwet, onderwijswetten etc..)
- Wet beveiliging netwerk- en informatiesystemen (Wbni) als Digitale Dienstverlener

Daarnaast zijn ook onderwijsstandaarden van toepassing, zoals de ROSA-katern IBP.

3.6. De vijf vuistregels van privacy en verantwoordingsplicht

Kennisnet houdt zich bij het verwerken van persoonsgegevens aan de beginselen rond de verwerking persoonsgegevens en kan dit ook aantonen (art.5 AVG). De **vijf vuistregels** van privacy zijn:

1. **Doel en doelbinding**: persoonsgegevens worden alleen gebruikt voor uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Deze doeleinden zijn concreet en voorafgaand aan de verwerking vastgesteld. Persoonsgegevens worden niet verder verwerkt voor andere doeleinden.
2. **Grondslag**: verwerking van persoonsgegevens is gebaseerd op een van de wettelijke grondslagen.
3. **Dataminimalisatie**: bij de verwerking van persoonsgegevens blijft de hoeveelheid en het soort gegevens beperkt. Het type persoonsgegevens staat in verhouding tot het doel – het doel kan niet met minder of alternatieve gegevens worden bereikt. Dit betekent ook dat data niet langer wordt bewaard dan noodzakelijk.
4. **Transparantie**: Kennisnet legt aan betrokkenen (zoals leerlingen, hun ouders en medewerkers) op transparante manier en ongevraagd verantwoording af over het gebruik van hun persoonsgegevens en het beleid daarover. Daarnaast hebben de betrokkenen recht op verbetering, aanvulling, verwijdering of afscherming van hun persoonsgegevens. Ook kunnen betrokkenen zich geheel verzetten tegen het gebruik van hun persoonsgegevens.
5. **Data-integriteit**: er zijn maatregelen getroffen om te waarborgen dat de te verwerken persoonsgegevens juist en actueel zijn.

Kennisnet neemt passende technische en organisatorische maatregelen om te waarborgen dat de persoonsgegevens op een passende wijze wordt beveiligd en worden beschermd tegen verlies, vernietiging, beschadiging of onrechtmatige verwerking.

3.7. Verwerkingsregister

Alle verwerkingen binnen en namens Kennisnet worden vastgelegd en up-to-date gehouden in een verwerkingsregister. Hierbij wordt onderscheid gemaakt tussen verwerkingen als ‘verantwoordelijke’ en als ‘verwerker’.

3.8. Planning & controle

Kennisnet doorloopt een jaarlijkse planning- en controlecyclus voor informatiebeveiliging, privacy en bedrijfscontinuïteit. Deze bestaat minimaal uit de volgende activiteiten:

- **Risicomanagement** is een continu proces binnen Kennisnet. Risico’s worden het gehele jaar geïdentificeerd, geanalyseerd, geavaleerd en beoordeeld. De resultaten hiervan bepalen welke informatiebeveiligings- en continuïteitsmaatregelen geïmplementeerd of verbeterd dienen te worden.
- **Controle en rapportage**
  - Operationele controle op de naleving van beleid en richtlijnen wordt verricht door het lijnmanagement. De CISO rapporteert aan het MT, de Directeur Operations (DO) over de informatiebeveiliging binnen Kennisnet, de vorderingen rond implementatie en verbetering van maatregelen en de incidenten in dat kwartaal. Dat geldt ook voor de acties die uit de risicobeoordeling zijn gekomen.
  - Interne audit: controle op de implementatie en borging van het beleid voor informatiebeveiliging, privacy en bedrijfscontinuïteit en de richtlijnen en maatregelen die hieruit voortkomen. Deze vindt gedurende het jaar plaats en wordt gedetailleerd beschreven in het ‘Auditprogramma ISMS’. Rapportage vindt plaats aan de CISO en DO.
  - Externe audit: minimaal jaarlijks een onafhankelijke controle van het ISMS en bijbehorende maatregelen. Rapportage vindt plaats aan de CISO en DO.

4. Organisatie

Kennisnet verdeelt de rollen en verantwoordelijkheden als volgt:

4.1. Medewerkers

Alle medewerkers hebben verantwoordelijkheid met betrekking tot informatiebeveiliging en privacy in hun dagelijkse werkzaamheden, zoals beschreven in het Personeelshandboek en de 'Aanvaardbaar gebruik van Bedrijfsmiddelen'. Daarnaast worden medewerkers in hun dagelijkse werkzaamheden, waar nodig, ondersteund.

Wij vragen medewerkers zich actief bezig te houden met informatiebeveiliging en privacy. Bijvoorbeeld door meldingen te maken van security incidenten of datalekken, verbetervoorstellen te doen en invloed uit te oefenen op het beleid binnen Kennisnet (individueel of via de OR).

4.2. Management

Het (lijn)management heeft een voorbeeldfunctie en draagt daarnaast een aantal verantwoordelijkheden:

- De bestuurder is de eindverantwoordelijke voor informatiebeveiliging, privacy en bedrijfscontinuïteit.
- Het MT is verantwoordelijk voor het vaststellen van het beleid (en de daaruit volgende richtlijnen) voor Kennisnet en ziet toe op de uitvoering ervan door het lijnmanagement. Binnen het MT is de Directeur Operations portefeuillehouder.
- Het lijnmanagement (zoals domeinmanagers en proceseigenaren) is verantwoordelijk voor de implementatie van het beleid binnen de organisatie en ziet erop toe dat dit door vaste en ingehuurde medewerkers wordt nageleefd.
- N.B. De CISO adviseert (on)gevraagd het (lijn)management over de implementatie van dit beleid.

4.3. Specifieke verantwoordelijkheden

Voor de uitvoering van het beleid voor informatiebeveiliging, privacy en bedrijfscontinuïteit zijn onder meer nodig: beleidsvoorbereiding, beheer van de processen, richtlijnen en procedures en controle op de naleving daarvan. Kennisnet verdeelt deze verantwoordelijkheden als volgt:

Rol/Functie	Verantwoordelijkheid
Directeur Operations	Beschikbaar stellen van de benodigde middelen, het belang van informatiebeveiliging, privacy en bedrijfscontinuïteit uitdragen en toezien op behalen de afgesproken doelstellingen. Daarnaast eigenaar van alle risico's binnen het ISMS.
CTO	Is verantwoordelijk voor het IT beleid en het ontwikkelproces.
CISO	Is verantwoordelijk voor het ISMS en onderhoudt het "Beleid voor informatiebeveiliging, privacy en bedrijfscontinuïteit" en het "Business Continuity Management System"
FG	Houdt toezicht op de naleving van de AVG en doet aanbevelingen voor bescherming van persoonsgegevens. De CISO en de FG zorgen voor een goede taakverdeling rond IBP.
Security Officer	Is verantwoordelijk voor het behandelen van securityincidenten en is het technische aanspreekpunt rond informatiebeveiliging binnen Kennisnet.
Interne Auditor	Voert de interne audit in een onafhankelijke positie uit conform het auditprogramma en legt bevindingen voor aan de CISO.
Domeinmanager Exploitatie	Houdt de centrale geautomatiseerde informatievoorziening en de beveiliging daarvan in stand.
Hoofd BHV	Is, wat informatiebeveiliging en privacy betreft, verantwoordelijk voor het duiden van veiligheidsvoorzieningen rond de (fysieke) veiligheid van Kennisnetmedewerkers.
Manager B&C	Is verantwoordelijk voor de fysieke beveiliging van het kantoorpand en de informatiebeveiliging rond administratieve procedures.
Manager P&O	Beheert het personeelsbeleid van Kennisnet. Dit raakt de informatiebeveiliging en privacy wat betreft de selectie, de voorlichting en het ontslag van personeel en het gebruik en delen van personeelsgegevens.
Servicedesk medewerkers	Beheren het loket voor inzageverzoeken en meldingen van externe partijen.