

Beveiligingsbeleid Stichting Kennisnet

AAN

VAN

Jerry van de Leur (Security Officer)

DATUM

ONDERWERP

Beveiligingsbeleid Stichting Kennisnet

Disclaimer:

Kennisnet geeft geen enkele garantie, met betrekking tot de geschiktheid voor een specifiek gebruiksdoel, functionaliteit en/of bruikbaarheid van de gepubliceerde informatie. De gepubliceerde documenten zijn ontwikkeld voor de specifieke situatie van Kennisnet als internetorganisatie. Kennisnet aanvaardt geen aansprakelijkheid voor schade ontstaan door het gebruik van deze informatie.

Inleiding

De missie van Kennisnet is het stimuleren van Internet gebruik in het onderwijs. Kennisnet voert deze missie uit door onder andere Internet diensten, bijvoorbeeld de Portals, Entree en Davindi, aan te bieden aan het onderwijs. Een belangrijke eigenschap van de Kennisnet diensten is dat deze betrouwbaar en veilig zijn: de Portals mogen bijvoorbeeld alleen informatie bevatten die geschikt zijn voor de doelgroepen en gebruikersgegevens dienen goed beveiligd te zijn.

Om deze betrouwbaarheid en veiligheid te waarborgen heeft Kennisnet een beveiligingsbeleid ingesteld. Dit beveiligingsbeleid beschrijft de eisen en verantwoordelijkheden die gesteld worden aan personeel en diensten van Kennisnet, om een goede beveiliging van de Kennisnet diensten te waarborgen. Het beveiligingsbeleid bestaat uit drie onderdelen: het beleid, een risicoanalyse methode en de security policy.

Het *Beleid* geeft de kaders en verantwoordelijkheden voor het beveiligingsbeleid bij Kennisnet. Met de *risicoanalyse methode* wordt het gewenste beveiligingsniveau van een dienst vastgesteld, de *security policy* bepaalt de beveiligingsmaatregelen die bij dat beveiligingsniveau horen.

Dit document bevat het *Beveiligingsbeleid van Stichting Kennisnet*.

Beveiligingsbeleid Stichting Kennisnet

Samenvatting

1. **Verantwoordelijkheid:** Informatie, applicaties, systemen en diensten binnen Kennisnet heeft/hebben altijd een eigenaar, deze eigenaar is verantwoordelijk voor de beveiliging ervan. Iedereen binnen Kennisnet is bijvoorbeeld verantwoordelijk voor de beveiliging van zijn/haar wachtwoorden en vertrouwelijke informatie. Productmanagers zijn verantwoordelijk voor de beveiliging van de diensten waarvoor zij verantwoordelijk zijn.
2. **Kennis:** medewerkers van Kennisnet zijn op de hoogte van het beveiligingsbeleid en handelen daarnaar. Hieronder valt bijvoorbeeld het 'locken' van werkstations bij afwezigheid, zorgvuldig omgaan met wachtwoorden en het opbergen van vertrouwelijke informatie.
3. **Externe partijen:** Activiteiten die zijn uitbesteed aan externe partijen moeten aan dezelfde beveiligingseisen voldoen als activiteiten die door Kennisnet zelf worden uitgevoerd
4. **Beveiliging van diensten:** voor elke dienst is een CIA-classificatie vastgesteld. De dienst voldoet aan de eisen die de security policy stelt voor deze CIA-classificatie.
5. **Privacy en vertrouwelijkheid:** alle Kennisnet diensten voldoen aan het Kennisnet handvest en aan relevante wet- en regelgeving.
6. **Misbruik:** de volgende activiteiten zijn expliciet verboden:
 - a. Het gebruiken van bedrijfsmiddelen voor andere activiteiten dan waarvoor deze bedoeld zijn
 - b. Het gebruiken en/of verspreiden van illegale content en applicaties
 - c. Het bewust verspreiden van computervirussen, *worms*, *trojan horses*, of andere kwaadaardige software
 - d. (proberen) toegang te krijgen en/of gebruiken van bedrijfsmiddelen waarvoor men niet geautoriseerd is
 - e. Het bewust toegankelijk maken van bedrijfsmiddelen voor ongeautoriseerde gebruikers
 - f. Het plaatsen van gevoelige of vertrouwelijke gegevens op computersystemen die niet afdoende zijn beveiligd
 - g. Het openbaar maken van gegevens waarvan men het recht niet heeft om deze gegevens openbaar te maken
7. **Wie doet wat?**
 - a. De CTO is eindverantwoordelijk voor het beveiligingsbeleid van Kennisnet
 - b. De Security Officer (SO) is verantwoordelijk voor het opstellen en implementeren van het beveiligingsbeleid, en voor het reageren op beveiligingsincidenten
 - c. De Manager PT&B is verantwoordelijk voor de beveiliging van de Kennisnet diensten en de kantoorautomatiseringsomgeving van Kennisnet.
8. **Wat te doen bij beveiligingsincidenten?** Waarschuw dan direct de volgende personen: je directe manager, de Security Officer en de Manager PT&B.

Algemeen

Elke gebruiker van Kennisnet is verantwoordelijk voor de beveiliging en bescherming van informatie, applicaties, systemen en diensten waarvan hij of zij de functioneel eigenaar is. De maatregelen omvatten bescherming tegen bedreigingen zoals ongeautoriseerde toegang, misbruik of ongeautoriseerde verandering. Activiteiten die uitbesteed zijn aan externe partijen moeten aan dezelfde beveiligingseisen voldoen als activiteiten die door Kennisnet zelf worden uitgevoerd.

Rollen en verantwoordelijkheden

Verantwoordelijkheden kunnen variëren van het beheren van de beveiliging van een groot systeem tot het beschermen van een wachtwoord. Hieronder worden de – voor beveiliging relevante - rollen beschreven die bij Kennisnet voorkomen, met de bijbehorende verantwoordelijkheden. Bij Kennisnet hebben de meeste medewerkers meerdere rollen.

Eigenaren van diensten zoals unitmanagers, sectormanagers en productmanagers zijn verplicht om:

- Diensten (inclusief alle bijbehorende gegevens) die onder hun controle vallen te identificeren
- Functie en doel van deze diensten en gegevens te bepalen en ervoor te zorgen dat er voldoende informatie beschikbaar is binnen de organisatie om de diensten doelmatig in te zetten
- Diensten voldoende te beveiligen. De mate van beveiliging wordt bepaald door factoren als:
 - Hoe betrouwbaar is de informatie die door de dienst wordt verwerkt?
 - Wordt het functioneren van Kennisnet negatief beïnvloed door het niet, of beperkt beschikbaar zijn van de informatie?
 - Wat is de schade voor Kennisnet bij aantasting van de integriteit van de informatie of het onbedoeld bekend worden van de informatie? (schade kan hierbij zowel financiële als imagoschade zijn)
 - Hoe waarschijnlijk is het dat een diensten of informatie kan worden gebruikt voor onrechtmatige activiteiten?
 - Welke limieten worden gesteld door beschikbare technologie, benodigde inspanning, kosten en beschikbare ondersteuning?
- Te controleren dat de benodigde beveiligingsmaatregelen correct zijn geïmplementeerd voor de betreffende diensten en gegevens

Providers zoals medewerkers die applicaties en systemen ontwerpen, bouwen en beheren (zoals project managers, system designers, developers, functioneel applicatiebeheerders en systeembeheerders) zijn verplicht om:

- Op de hoogte te zijn van relevante beveiligingseisen en –richtlijnen voor het ontwerpen, bouwen en beheren van applicaties en systemen
- Potentiële bedreigingen en de geschiktheid van de beveiligingsmaatregelen te analyseren en daarover te adviseren richting de Eigenaren van diensten die gebruik maken van deze applicaties en systemen.
- Voldoende beveiligingsmaatregelen te implementeren om bedreigingen te minimaliseren tot een aanvaardbaar risico. Het aanvaardbare risico wordt bepaald door de Eigenaren van de diensten die gebruik maken van deze applicaties en systemen.
- Alert en vakkundig te reageren op beveiligingsincidenten en maatregelen te nemen om te voorkomen dat een soortgelijk incident in de toekomst nogmaals voorkomt.

- Procedures in te richten en te onderhouden met het doel het aantal accounts met speciale bevoegdheden tot een minimum te beperken en dat eigenaren van deze accounts zich houden aan de eisen die aan het gebruik van dergelijke accounts worden gesteld.
- Duidelijk te communiceren over de doelen en gebruiksregels voor applicaties en systemen die onder hun controle vallen

Gebruikers die toegang hebben tot- en gebruik maken van applicaties en systemen, zijn verplicht om:

- Op de hoogte te zijn van relevante beveiligingseisen en –richtlijnen voor het gebruiken van deze applicaties en systemen
- Applicaties en systemen die onder hun controle vallen te beschermen. Hieronder valt ook bescherming van gevoelige gegevens (bv. wachtwoorden, configuratieinformatie) over deze systemen.

De **CTO** is eindverantwoordelijk voor het beveiligingsbeleid van Kennisnet. Het beveiligingsbeleid regelt informatiebeveiliging en beveiliging van de Kennisnet diensten.

De **Security Officer (SO)** De Security Officer (SO) is verantwoordelijk voor het opstellen en implementeren van het beveiligingsbeleid, en voor het reageren op beveiligingsincidenten

De **Manager Portal Techniek & Beheer** is verantwoordelijk voor de beveiliging van de Kennisnet diensten en de kantoorautomatiseringsomgeving van Kennisnet

Onvoldoende beveiligingsmaatregelen kunnen ertoe leiden dat applicaties, systemen of diensten worden beschadigd, gestolen of een aansprakelijkheid opleveren voor Kennisnet. Kennisnet kan dan ook maatregelen nemen om dit soort gebeurtenissen tegen te gaan. Voorbeelden van dit soort maatregelen zijn het blokkeren van Internet toegang of het blokkeren van accounts. De CTO bepaalt welke maatregelen worden genomen in specifieke situaties.

Beveiligingselementen

Logische beveiliging

Computersystemen en software moeten steeds worden voorzien van de meest recente, relevante software security patches. Het beveiligingsniveau moet voldoende zijn om bedreigingen terug te brengen tot het van tevoren bepaalde aanvaardbare risico. Computersystemen die direct gekoppeld zijn aan het Internet (vooral servers) dienen met extra zorg te worden behandeld. Tevens moeten voldoende authenticatie- en autorisatiemaatregelen worden geïmplementeerd.

Niet alleen grote computersystemen en infrastructures, maar ook kleinere computers en portable devices die gevoelige informatie kunnen bevatten (zoals laptops, blackberry's) moeten voldoende worden beveiligd.

Fysieke beveiliging

Er moeten voldoende beveiligingsmaatregelen worden geïmplementeerd om fysieke toegang tot informatie, applicaties en systemen te beperken. Het beveiligingsniveau moet voldoende zijn om bedreigingen terug te brengen tot het van tevoren bepaalde aanvaardbare risico. Deze maatregelen kunnen variëren van toegangsbeveiliging tot datacenter ruimtes tot password-protected screensavers.

Vaststellen van het beveiligingsniveau

De **Kennisnet security policy** bevat de benodigde maatregelen om een beveiligingsniveau te creëren waarmee bedreigingen terug te kunnen brengen tot een aanvaardbaar risico. De Security Officer is verantwoordelijk voor de security policy.

Het aanvaardbare risico wordt bepaald door de CIA-classificatie (Confidentiality, Integrity, Availability) van het bedrijfsmiddel. De Eigenaar van het bedrijfsmiddel is verantwoordelijk voor het vaststellen van de CIA-classificatie. Binnen Kennisnet wordt een **risicoanalyse methode** gebruikt om deze CIA-classificatie vast te stellen.

Privacy en vertrouwelijkheid

Computersystemen en software die ingezet worden voor diensten moeten zodanig worden ontwikkeld en gebruikt dat de privacy en vertrouwelijkheid van gegevens, die door die software en computersystemen worden verwerkt, gewaarborgd is en voldoet aan relevante wet- en regelgeving en de Kennisnet security policy.

Gebruikers die geautoriseerd zijn om gegevens te benaderen dienen ervoor te zorgen dat deze gegevens afdoende beschermd zijn en dat daarbij wordt voldaan aan relevante wet- en regelgeving en de Kennisnet security policy.

Medewerkers die technisch beheer uitvoeren op Kennisnet systemen en daarvoor accounts hebben met speciale bevoegdheden, zijn niet bevoegd om gegevens, elektronische communicatie en daaraan gerelateerde transacties te bekijken of te doorzoeken, zonder dat daarvoor een wettelijke grondslag bestaat.

Misbruik

Kennisnet keurt versturende of illegale activiteiten op het Internet, zoals het verspreiden van virussen en spam, af en neemt maatregelen om te voorkomen dat dergelijke activiteiten vanaf, of via de systemen van Kennisnet worden uitgevoerd.

De volgende activiteiten zijn expliciet verboden:

- Het ondoelmatig gebruik en het verstoren van bedrijfsmiddelen
- Het bewust verspreiden van computervirussen, *worms*, *trojan horses*, of andere kwaadaardige software
- Onderzoeken van, pogingen ondernemen om toegang te krijgen tot, toegang krijgen tot of gebruiken van bedrijfsmiddelen waarvoor men niet geautoriseerd is
- Het bewust toegankelijk maken van bedrijfsmiddelen voor ongeautoriseerde gebruikers

- Het downloaden van gevoelige of vertrouwelijke gegevens naar computersystemen die niet afdoende zijn beveiligd tegen ongeautoriseerde toegang
- Het openbaar maken van gegevens waarvan men het recht niet heeft om deze gegevens openbaar te maken.

Relevante wet- en regelgeving en security policy

Alle bedrijfsmiddelen van Kennisnet, en alle werkzaamheden die aan of met behulp die bedrijfsmiddelen worden uitgevoerd, dienen in overeenstemming te zijn met de wet- en regelgeving. De volgende wetten en regelgeving is relevant voor Kennisnet:

- De Wet Bescherming Persoonsgegevens (WBP)
- Voorschrift Informatiebeveiliging Rijksoverheid (VIR)
- Het Handvest van Kennisnet

Ondertekening

De Directeur en CTO van Kennisnet verklaren dit Beveiligingsbeleid actief te ondersteunen en uit te voeren:

Directeur Kennisnet	CTO Kennisnet
Plaats:	Plaats:
Datum:	Datum:
Naam:	Naam:
Handtekening:	Handtekening: