TYPE PUBLICATIE
Publiek

| | |
|---|---|
| VERANTWOORDELIJKE | **DUTRIEUX Thibault** |
| PUBLICATIEDATUM | 16-02-26 |
| VERVALDATUM | 15-02-28 |
| VERSION | 1.4 |

# Gebruiksvoorwaarden KEYES-Online Services

## 1 Doel

Dit document is opgesteld om de gebruiksvoorwaarden vast te leggen van de online services die KEYES aan zijn Klanten aanbiedt.

Deze voorwaarden regelen het gebruik van de Online Services van KEYES door de Klant en de verplichtingen van de Klant en KEYES met betrekking tot de verwerking en beveiliging van Klantgegevens en Persoonsgegevens.
De algemene aankoopvoorwaarden van de Klant voor onlinediensten zijn uitdrukkelijk uitgesloten voor het gebruik van de Online Services van KEYES, tenzij KEYES vooraf schriftelijke toestemming heeft gegeven.

## 2 Definities

**Klant:** iedere entiteit die met KEYES een overeenkomst heeft gesloten voor de uitvoering van de Online Services van KEYES.

**Klantgegevens:** alle gegevens, waaronder begrepen tekst-, geluids-, video- of beeldbestanden en software die door of namens de Klant in verband met het gebruik van de Online Services van KEYES worden verstrekt.

**Persoonsgegevens**: alle informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon (hierna "betrokkene" genoemd). Een "identificeerbare natuurlijke persoon" is iemand die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator, zoals een naam, een identificatienummer, locatiegegevens, een online inlognaam, of van een of meer specifieke elementen die kenmerkend zijn voor zijn fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit.

**DPO**: Data Protection Officer.

**Beveiligingsincident:** een inbreuk op de beveiliging die resulteert in vernietiging, verlies, wijziging, niet-geautoriseerde bekendmaking van of toegang tot Klantgegevens of Persoonsgegevens, op accidentele of onwettige wijze.

**KEYES**: wordt verstaan als Network Research Belgium nv, evenals haar huidige en toekomstige vestigingen in België en in het buitenland.

**Online Services van KEYES**: Elke onlinedienst die KEYES onder contract aan zijn Klanten ter beschikking stelt.

**Gebruiker:** elke natuurlijke of rechtspersoon die onder controle van de Klant staat en toegang heeft tot de online services van KEYES. In de context van sommige diensten kan een computer of robot die toegang heeft tot de dienst ook als "Gebruiker" worden beschouwd.

# 3 Toepassingsgebied

De genoemde voorwaarden zijn van toepassing op alle Online Services van KEYES. Deze omvatten (maar zijn niet beperkt tot):

- De NECS-service, waarvan de verschillende toepassingen toegankelijk zijn via het NECS-portaal.
- De SIEM/SOC-service gebaseerd op Splunk.

# 4 Naleving van wet- en regelgeving

KEYES verplicht zich tot naleving van alle wet- en regelgeving die van toepassing is op het aanbieden van de Online Services van KEYES, waaronder wetgeving met betrekking tot de melding van beveiligingslekken en de verplichtingen tot bescherming van persoonsgegevens. KEYES is echter niet verantwoordelijk voor de naleving van enige wet- of regelgeving die van toepassing is op de Klant of de sector van de Klant die niet algemeen van toepassing is op IT-dienstverleners. KEYES bepaalt niet of de Klantgegevens informatie bevatten waarop een specifieke wet of regeling van toepassing is. Voor alle Beveiligingsincidenten gelden de volgende bepalingen over de Meldingen van Beveiligingsincidenten (MBI).

De Klant is verplicht om alle wetten en voorschriften die op zijn gebruik van de Online Services van KEYES van toepassing zijn, met inbegrip van de wetten betreffende de vertrouwelijkheid van communicatie, de AVG, alsmede de verplichtingen inzake de bescherming van persoonsgegevens van de AVG. Het is de verantwoordelijkheid van de Klant om te bepalen of de Online Services van KEYES geschikt zijn voor de opslag en verwerking van informatie die onderworpen is aan enige specifieke wet- of regelgeving en om de Online Services van KEYES te gebruiken op een wijze die in overeenstemming is met de wettelijke en regelgevende verplichtingen van de Klant.

Het is de verantwoordelijkheid van de Klant om te reageren op elk verzoek van een derde met betrekking tot het gebruik van een Online Service van KEYES door de Klant, zoals een verzoek om toegang tot de inhoud door een Belgische gerechtelijke instantie.

# 5 Gebruik van Online Services van KEYES

De Klant is gemachtigd om de Online Services van KEYES te gebruiken in overeenstemming met zijn contract en deze gebruiksvoorwaarden. KEYES behoudt zich het recht voor commercieel redelijke wijzigingen aan te brengen in elke Online Service van KEYES.

## 5.1 Verantwoordelijkheden van de Klant

**Gebruik van Online Services van KEYES**
De Klant is verantwoordelijk voor zijn transacties en het gebruik dat hij of zijn Gebruikers maken van de Online Services van KEYES. De Klant waakt erover dat dit gebruik van de Online Services van KEYES geschiedt in overeenstemming met de overeenkomst en deze gebruiksvoorwaarden. Hij is er verantwoordelijk voor dat het doel, de reikwijdte en de kenmerken van de Online Services van KEYES voldoen aan de eisen en behoeften die hij in zijn lastenboek/RFP heeft geformuleerd.

**Gebruikers**
De Klant is verantwoordelijk voor het identificeren en authenticeren van zijn Gebruikers, het goedkeuren van de toegang van deze Gebruikers tot de Online Services van KEYES, het controleren van onbevoegde toegang en het handhaven van de vertrouwelijkheid van gebruikersnamen, wachtwoorden en accountinformatie. KEYES is niet aansprakelijk voor schade veroorzaakt door de Klant en de Gebruikers, waaronder de personen die geen toegang hebben tot de Online Services van KEYES. De Klant is als enige verantwoordelijk voor het gebruik van de Online Services van KEYES door zijn Gebruikers of personen die gebruik maken van zijn gebruikersaccounts.
Indien Gebruikers technisch worden beheerd door KEYES, is de Klant verplicht KEYES te informeren, zodra hij op de hoogte is van enige wijziging met betrekking tot zijn Gebruikers (vertrek, mobiliteit of anderszins).

**Veiligheidsverplichtingen**
De Klant is als enige verantwoordelijk om zelfstandig vast te stellen of de technische en organisatorische maatregelen van een Online Service van KEYES voldoen aan de eisen van de Klant, met inbegrip van zijn beveiligingsverplichtingen uit hoofde van de toepasselijke verplichtingen inzake de bescherming van persoonsgegevens. De Klant erkent en aanvaardt dat (rekening houdend met de huidige stand van de kennis, de kosten van de tenuitvoerlegging en de aard, de omvang, de context en de doeleinden van de verwerking van zijn Persoonsgegevens alsmede de risico's voor personen) de door KEYES ingevoerde en gehandhaafde beveiligingspraktijken en -strategieën een beveiligingsniveau garanderen dat in verhouding staat tot het risico met betrekking tot zijn Persoonsgegevens. De Klant is volledig verantwoordelijk voor het implementeren en onderhouden van beveiligings- en beschermingsmaatregelen voor persoonsgegevens voor componenten die de Klant levert of beheert (zoals een virtuele machine of applicatie die de Klant gebruikt op het NECS-platform).

## 5.2 Regels voor goede gebruikspraktijken

De Klant, noch iemand die toegang heeft tot een Online Service van KEYES is bevoegd voor het gebruik van een Online Service van KEYES:

- in strijd met wetten, verordeningen of voorschriften, of in strijd met de rechten van anderen;

- om te proberen onbevoegde toegang te krijgen tot diensten, apparaten, gegevens, accounts of netwerken of deze te verstoren;
- om ongewenste e-mails te versturen of malware te verspreiden;
- op een manier die de Online Service van KEYES kan beschadigen of het gebruik ervan door een andere gebruiker kan verstoren;
- in elke toepassing of situatie waarin het falen van de Online Service van KEYES de dood of ernstig lichamelijk letsel van enige persoon, dan wel ernstige fysieke of milieuschade tot gevolg kan hebben; of
- om eender welke persoon te helpen of aan te moedigen om bovenvermelde acties uit te voeren.

Schending van deze regels van goede gebruikspraktijken kan leiden tot schorsing van de Online Service van KEYES. KEYES zal de Klant voorafgaand aan een eventuele schorsing van een Online Service van KEYES om bovengenoemde redenen op de hoogte stellen, behalve indien KEYES een onmiddellijke schorsing noodzakelijk acht.

## 5.3 Technische beperkingen

De Klant moet zich houden aan de technische beperkingen die van toepassing zijn op een KEYES Online Service en mag deze niet omzeilen. Het gebruik van de functies door de klant moet in overeenstemming zijn met hetgeen door KEYES is bepaald. KEYES kan niet aansprakelijk worden gesteld voor het verdwijnen van niet-gedocumenteerde functies, of voor evoluties daarvan die een impact hebben op het gebruik door de klant en die een afwijking vormen van het oorspronkelijke doel ervan.

## 5.4 Beschikbaarheid

De beschikbaarheid van elke Online Service van KEYES en zijn functionaliteiten wordt niet gegarandeerd, tenzij in het tussen KEYES en de Klant geldende contract uitdrukkelijk een niveau van beschikbaarheid is vastgelegd.

# 6 Bescherming van gegevens en beveiliging

KEYES verplicht zich alle redelijke maatregelen te nemen om een adequaat beveiligingsniveau te bieden bij het aanbieden van de Online Services van KEYES. Als zodanig ontwikkelt en onderhoudt KEYES een gedocumenteerd Information Security Management System (ISMS) gebaseerd op de norm ISO27001:2022.

In de bijlage "Standaard technische en organisatorische beveiligingsmaatregelen" worden de technische en organisatorische beveiligingsmaatregelen die van toepassing zijn op de Online Services van KEYES nader beschreven. Deze bijlage is beschikbaar op het portaal met de documentatie voor de klant.

De Klant verplicht zich KEYES zo spoedig mogelijk op de hoogte te stellen van een beveiligingsincident dat de Online Services van KEYES of de door KEYES gehoste gegevens van de Klant aantast.

# 7 Melding van Beveiligingsincidenten

Als KEYES kennis krijgt van een Beveiligingsincident tijdens de verwerking van Klantgegevens of Persoonsgegevens door KEYES, zal KEYES onverwijld en zonder vertraging:
(1) de Klant in kennis stellen van het Beveiligingsincident;
(2) het Beveiligingsincident onderzoeken en de Klant hierover informatie verstrekken; en
(3) redelijke maatregelen nemen om de gevolgen van het veiligheidsincident in te dammen en de nadelige gevolgen ervan zoveel mogelijk te beperken.

Kennisgevingen van Beveiligingsincidenten worden verzonden aan een of meer beheerders van de Klant, op een door KEYES te kiezen wijze, waaronder per e-mail. Kennisgevingen van Beveiligingsincidenten met betrekking tot Persoonsgegevens zullen ook aan de DPO van de Klant worden gestuurd, op een door KEYES gekozen wijze, waaronder per e-mail.

Het is uitsluitend de verantwoordelijkheid van de Klant om ervoor te zorgen dat updates van de contactgegevens van zijn bestuurders en de DPO aan KEYES worden doorgegeven. De Klant is als enige verantwoordelijk voor de naleving van zijn verplichtingen uit hoofde van de wetten over de melding van incidenten die op de Klant van toepassing zijn en voor de naleving van eventuele meldingsverplichtingen aan derden in verband met een Beveiligingsincident.

KEYES zal redelijke inspanningen verrichten om de Klant bij te staan bij het vervullen van zijn verplichting om de bevoegde autoriteiten en de betrokken personen in kennis te stellen van dit Beveiligingsincident, krachtens artikel 33 van de AVG of andere toepasselijke wet- of regelgeving.

De reactie van KEYES op of kennisgeving van een Beveiligingsincident uit hoofde van dit artikel houdt niet in dat KEYES enige fout of aansprakelijkheid met betrekking tot het Beveiligingsincident erkent.

De Klant moet KEYES zo snel mogelijk op de hoogte stellen in geval van mogelijk misbruik van zijn accounts of identificatiegegevens, of van een Security Incident met betrekking tot een Online Service van KEYES.

# 8 Specifieke voorwaarden voor bepaalde Online Services van KEYES

## NECS-service

**Definities:**

- CMP: Cloud Management Platform. Deze software is de hoeksteen van de cloud. Ze bestaat uit twee delen: de webinterface die de dienstencatalogus presenteert en de workflowmotor die de

automatische acties opeenvolgt en stap voor stap valideert. Ze koppelt en stuurt de verschillende infrastructuurcomponenten aan om de door u bestelde dienst te leveren.

- Tenant: Verwijst naar de cloud waarin uw systemen en gegevens zijn opgeslagen. Zo heeft elke Klant zijn eigen cloud, zijn eigen tenant, volledig geïsoleerd van andere Klanten.

**Beheer van licenties en ongeoorloofd gebruik of ongeoorloofde inhoud**
Indien de Klant applicaties/software installeert of gebruikt op de door KEYES ter beschikking gestelde infrastructuur, dient de Klant zich te houden aan de bepalingen van het softwarelicentiebeheer-platform (Software Licensing Management Services), beschikbaar op www.keyes.eu, die in het contract zijn opgenomen.

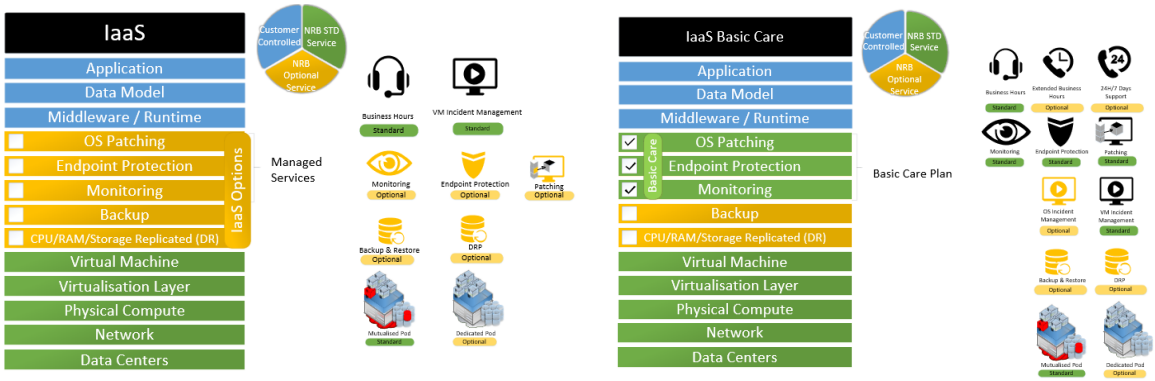
**Gebruik van niet-ondersteunde componenten**
Indien de Klant op de door KEYES geleverde infrastructuur componenten installeert of gebruikt die niet door derde leveranciers worden ondersteund (bijvoorbeeld een OS dat niet meer door de leverancier wordt ondersteund), neemt de Klant hiervoor de volledige verantwoordelijkheid op zich en ontslaat hij KEYES van alle verplichtingen ten aanzien van naleving van SLA's, kwaliteit of beveiliging.

**Toegang tot persoonsgegevens**
Binnen CMP hebben alle gebruikers in dezelfde Tenant, toegang tot de volgende persoonsgegevens van andere gebruikers van de Tenant: Naam, voornaam, e-mail en zakelijk telefoonnummer. Het is de verantwoordelijkheid van de Klant die eigenaar is van de Tenant om ervoor te zorgen dat deze bepaling in overeenstemming is met zijn privacybeleid en dat van zijn leveranciers.

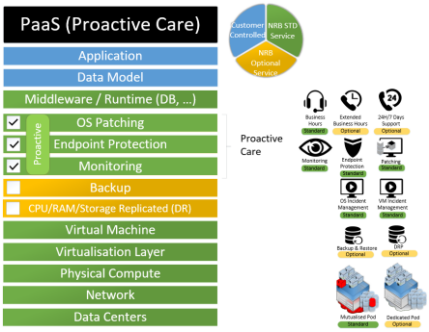
**Systeemconfiguratie Dual-Homed**
Binnen zijn Tenant heeft de Klant de mogelijkheid om Dual-Homed-systemen te configureren, d.w.z. met meerdere netwerkkaarten die op verschillende netwerksegmenten zijn aangesloten. Dit type configuratie kan het netwerkverkeer tussen netwerksegmenten met verschillende beveiligingsniveaus mogelijk maken zonder dat de firewall van de Tenant wordt gepasseerd. Indien de Klant een dergelijke configuratie gebruikt, neemt die de volledige verantwoordelijkheid daarvoor op zich en ontslaat hij KEYES van alle verplichtingen met betrekking tot de naleving van de SLA's, kwaliteit of beveiliging.

**Systemen beheren op een publieke cloud**
Met behulp van het CMP kan de Klant resources aanmaken en beheren op een andere publieke cloud dan de KEYES Cloud (Microsoft Azure en Amazon Web Services). Voor deze resources die gehost worden op een publieke cloud gelden de contracten, gebruiksvoorwaarden en SLA's die specifiek zijn voor de desbetreffende publieke cloud en niet de contracten, gebruiksvoorwaarden en SLA's van KEYES. Het is daarom de verantwoordelijkheid van de Klant om ervoor te zorgen dat het gebruik van de Public Cloud via het CMP voldoet aan de voor de Klant geldende wet- en regelgeving.

**Verdeling van verantwoordelijkheden tussen de Klant en KEYES**
De rollen en verantwoordelijkheden van elk zijn afhankelijk van het serviceniveau dat door de Klant is besteld en worden in de volgende diagrammen samengevat:




Indien KEYES zorg draagt voor OS Patching, Endpoint protection en/of Monitoring wordt een impact op de "Customer Controlled" lagen niet kosteloos door KEYES ondersteund.




Bovendien is de Klant volledig verantwoordelijk voor het beheer van de volgende elementen:

- Gebruikersbeheer in de Cloud Management Portal.
- Beheer van patchperiodes in de tegel 'Tenant Master Data & Networks'.
- Beheer van alle containers op een Red Hat OpenShift cluster gecreëerd door de Klant.
- Beheer van Load Balancers (F5 BIG-IP VE) & Centralized Management (BIG-IQ) aangemaakt door de Klant.
- Beheer van het beveiligingsbeleid van de VLAN's van de Tenant via de tegel 'Firewall Rules & Configuration' als de klant lees-/schrijftoegang nodig heeft.