



Beveiligingsbeleid

Inhoudsopgave

1. Introductie	4
1.1 Doel	4
1.2 Functionaliteiten	4
1.3 Wet- en regelgeving	4
1.4 Aanvullende documenten	4
1.5 Contactgegevens	5
2. Server	5
2.1 Programmatuur	7
2.2 Updates	7
2.3 Datacentrum	7
2.4 Toegankelijkheid	7
3. OTAP (DTAP)	8
3.1 Ontwikkelen	8
3.2 Testen	8
3.3 Acceptatie	8
3.4 Productie	8
4. Database	10
4.1 Toegankelijkheid	10
4.2 Back-up	10
5. Applicatie	11
5.1 Accounts, login, wachtwoorden en single sign-on	11
5.1.1 Nieuwe gebruikers	11
5.1.2 Single sign-on (SSO)	11
5.1.3 Login	12
5.1.4 Wachtwoorden	12
5.1.5 Sessions	13
5.1.6 Verwijderen van gebruikers	13
5.2 Afscherming en rollen	14
5.2.1 Afscherming per klant	14
5.2.2 Rollen en rechten van gebruikers	14
5.3 Encryptie	14
5.4 Foutafhandeling	15
5.5 Browsers & devices	15
5.5.1 Browsers	15
	2

5.5.2 Tablets	15
5.5.3 Mobiel	15
5.5.4 Devices ‘van de zaak’ en interne beveiligingsmaatregelen klanten	16
6. Testen en analyses	17
6.1 Penetratietesten	17
6.2 Loadtesting	17
6.4 Risico analyse organisatie en informatiebeveiliging	18
7. Subverwerkers	19
8. Sourcecode	20
8.1 Git	20
8.2 Cloud	20
8.3 Toegankelijkheid	20
9. Releasebeleid	21
10. Product Development team	22

1. Introductie

Dit Beveiligingsbeleid geldt voor het Online platform van Dialog, gebouwd door Dialog B.V. (hierna: Dialog). Dialog is geregistreerd bij de Kamer van Koophandel onder nummer 84510722.

1.1 Doel

Het Online platform ondersteunt medewerkers, leidinggevenden en HR om het goede gesprek te voeren over doelstellingen en ontwikkeling. Door het voeren van het goede gesprek dragen medewerkers optimaal bij aan het succes van de organisatie.

1.2 Functionaliteiten

Het Online platform faciliteert onder andere de volgende functionaliteiten:

- Het vastleggen en bijhouden van de voortgang op doelstellingen op organisatie, team/afdeling en individueel niveau;
- Feedback vragen en geven aan collega's en externen;
- Periodieke evaluaties invullen over en door een medewerker;
- Dashboards over de voortgang op doelstellingen en over het gebruik van het platform;
- Engagement metingen
- Talent in de organisatie in kaart brengen en ontwikkeling stimuleren
- Beheerschermen om het bovenstaande als Beheerder binnen een organisatie te kunnen beheren.

1.3 Wet- en regelgeving

Als ontwikkelaars hebben we uiteraard alle maatregelen genomen om aan de wet- en regelgeving te voldoen. Hiernaast hanteren we (het Product Development-team van Dialog) eigen procedures om de veiligheid van vastgelegde informatie en de stabiliteit van de applicatie te waarborgen.

1.4 Aanvullende documenten

Aanvullende documentatie naast dit Beveiligingsbeleid:

- Privacybeleid
- Privacyverklaring
- Cookiebeleid
- Service Level Agreement (SLA)
- Verwerkersovereenkomst
- Single Sign-On document

Vanuit dit Beveiligingsbeleid kan worden doorverwezen naar de bovenstaande documentatie. De bovenstaande documenten kunnen te allen tijde worden opgevraagd bij Dialog.

1.5 Contactgegevens

Kantoor Dialog

Weg der Verenigde Naties 1

3527 KT, Utrecht

Nederland

T: 030 7600 290 (Maandag t/m vrijdag, 09.00 - 17.00 uur)

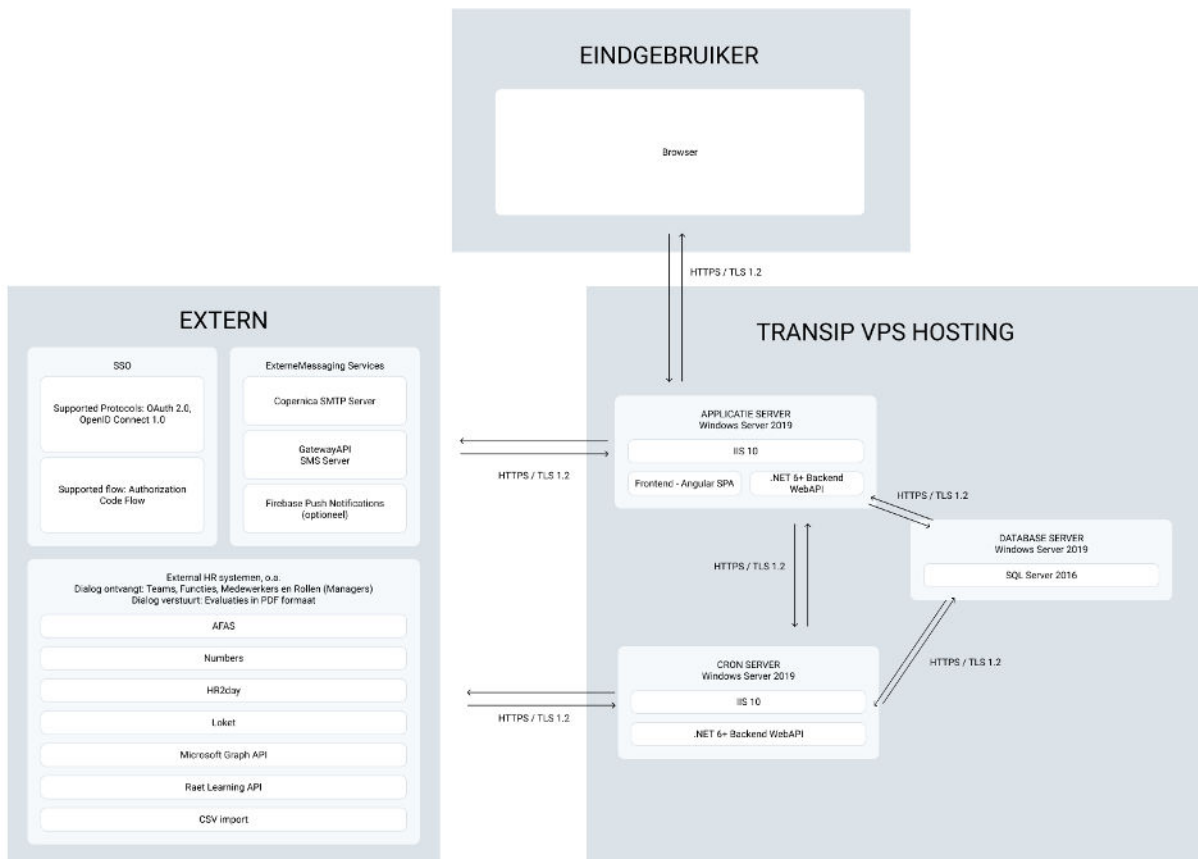
E: support@dialog.nl

2. Server

Het Online platform draait op 3 Virtual Private Servers van TransIP (<https://www.transip.nl/>). Het beheer van deze servers is in handen van de Lead Developer van Dialog. Medewerkers van TransIP hebben geen toegang tot de operationele zijde van het Online platform.

De 3 Virtual Private Servers hebben de volgende verantwoordelijkheden:

1. Database server met Microsoft SQL Server 2016;
2. Applicatie server met IIS 10 voor zowel de back-end, als de front-end;
3. Hangfire (cron job) server met IIS 10 voor de back-end.



Afbeelding 1: Architectuur

Dialog behoudt het recht om medewerkers van TransIP toegang tot de server te verlenen indien dit nodig is vanuit een technische behoefte, zoals server support.

2.1 Programmatuur

De servers draaien op Microsoft Windows Server 2019 Standard met uiterst geringe features. Vrijwel alle programmatuur is onderdeel van het Microsoft server platform, zoals IIS. De webserver staan direct op het internet zonder DMZ of WAP.

Daarnaast zijn de servers voorzien van een firewall (Windows Firewall met advanced security) waarmee de onnodige poorten worden geblokkeerd. Poorten 80 en 443 zijn gewhitelist in onze firewall.

2.2 Updates

De productieservers worden de 4de zondag van de maand automatisch voorzien van de laatste updates. Updates worden vooraf op de 2de en 3de zondagen van de maand geïnstalleerd op respectievelijk onze test en acceptatie omgevingen. Dit geeft ons de kans om te controleren dat updates geen invloed hebben op de beschikbaarheid en beveiliging van de productieservers. Kritieke beveiligingsupdates worden binnen twee werkdagen geïnstalleerd.

2.3 Datacentrum

Het datacentrum is in handen van The Datacenter Group te Amsterdam. Het datacentrum heeft 24/7 on-site bewaking, biometrische identificatie en een HD CCTV netwerk.

De virtual private servers worden iedere 4 uur gebackupt en off-site opgeslagen op een andere availability zone.

Het datacentrum is ISO 9001, ISO 27001 en ISO 14001 gecertificeerd. Daarmee zijn kwaliteits-, beveiligings- en milieumanagement optimaal gewaarborgd.

2.4 Toegankelijkheid

Er zijn verschillende maatregelen genomen om de toegankelijkheid tot databases en servers te beperken.

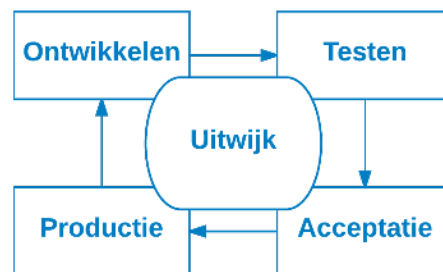
- Het datacentrum is onbereikbaar voor onbevoegden.
- De servers zijn via een Remote Desktop verbinding beperkt beschikbaar.
- De RDP server is uitsluitend extern benaderbaar voor een zeer kleine lijst aan gewhiteliste IP-adressen.
- Uitsluitend de lead developer van het Product Development-team heeft toegang tot de servers. De lead developer gebruikt deze toegang uitsluitend voor onderhouden van de servers, het release van nieuwe versies van het platform en het oplossen van problemen. Indien nodig wordt op een need-to-know basis tijdelijk toegang verleend aan een andere developer. Deze toegang wordt zo snel mogelijk weer ingetrokken.
- Via Windows Event Logs wordt bijgehouden welke login pogingen er worden gedaan op de server.
- Gefaalde login pogingen op de servers worden doorgestuurd per e-mail naar onze support inbox (support@dialog.nl). Tegelijkertijd wordt er een bericht gestuurd naar ons error logging Slack-kanaal. Beide worden tijdens werktijden actief gemonitord.

3. OTAP (DTAP)

Bij het ontwikkelen en onderhouden van het Online platform wordt gebruikt gemaakt van aparte omgevingen.

3.1 Ontwikkelen

Developers werken op een lokale ontwikkelomgeving op de computer van de developer aan nieuwe of verbeterde functionaliteiten. Eventuele bugs worden ook op deze lokale omgeving opgelost. Developers mogen zelf kiezen of zij op het Dialog kantoor in Utrecht of vanuit thuis werken.



Nieuwe of verbeterde functionaliteiten worden als deze klaar zijn allereerst gedemonstreerd aan de interne test specialist en vervolgens gedemonstreerd aan de designer(s) en product owner. Bij beide demonstraties worden eventuele verbeteringen direct doorgevoerd.

Als laatste stap wordt de opgeleverde broncode gereviewd door een andere developer en eventuele wijzigingen nog doorgevoerd.

3.2 Testen

Nieuwe versies van het Online platform worden altijd naar de testomgeving (staging) gebracht. Hier worden alle functionaliteiten van het Online platform uitvoerig getest (gebruikersacceptatie testen, regressietesten en geautomatiseerde testen). Deze testomgeving draait op een VPS met een fictieve database. Deze database staat compleet los van de productiedatabase.

3.3 Acceptatie

Op de acceptatieomgeving worden nieuwe functionaliteiten nog getest door Implementatiemanagers en (optioneel) door klanten. Dit gebeurt pas nadat de nieuwe release naar de productieomgeving wordt gebracht. Op deze omgeving worden ook beheer sessies e.d. gehouden, zodat beheerders kunnen rondklikken en experimenteren zonder dat dit gevolgen heeft voor een eindgebruiker. Op de acceptatieomgeving staat productiedata en er gelden dezelfde beveiligingsmaatregelen als op onze productieomgeving.

3.4 Productie

Na uitvoerig testen wordt de release candidate build op een gunstig tijdstip gereleased naar de productieomgeving. Dit is de live omgeving waar klanten en eindgebruikers op werken.

Meer informatie over ons releasebeleid, is terug te vinden in het SLA (Service Level Agreement) document.

Er is geen automatische synchronisatie tussen de vier verschillende omgevingen. Het zijn losse omgevingen die niet van elkaar afhankelijk zijn.

Er wordt geen data uitgewisseld tussen de ontwikkel- en testomgeving enerzijds en de productie- en acceptatieomgeving anderzijds. De databaseversies zijn uiteraard wel hetzelfde. Hierdoor wordt de kans op bugs verkleind.

4. Database

Het Online platform maakt gebruik van een instantie van SQL Server 2016. De database server wordt niet gebruikt voor andere applicaties en/of doeleinden.

4.1 Toegankelijkheid

Uitsluitend de lead developer van het Product Development-team heeft toegang tot de ongepseudonimiseerde productiedatabase met schrijfrechten. De lead developer gebruikt deze database uitsluitend voor het oplossen van klantproblemen die niet op te lossen zijn met een database met fictieve data. Indien nodig wordt op een need-to-know basis tijdelijk toegang verleend aan een andere developer. Deze toegang wordt zo snel mogelijk weer ingetrokken.

4.2 Back-up

Er wordt elke dag een back-up gemaakt van de Productiedatabase. Dit gebeurt 's nachts en volledig automatisch.

De back-ups van de Productiedatabase worden opgeslagen op Cloud Storage, gehost door Amazon Web Services (AWS). Voordat deze back-ups worden opgeslagen bij AWS, worden deze ge-encrypt. Hier wordt AES-256 encryptie toegepast. Back-ups worden niet geanonimiseerd.

De servers waar deze back-ups worden opgeslagen, staan in Frankfurt, Duitsland. De opgeslagen back-ups verlaten de EU niet.

Back-ups worden na 60 dagen na aanmaken automatisch verwijderd van de Cloud Storage dienst.

5. Applicatie

5.1 Accounts, login, wachtwoorden en single sign-on

5.1.1 Nieuwe gebruikers

Iedere gebruiker heeft een eigen account in het Online platform. Dit account is uitsluitend toegankelijk wanneer de juiste gebruikersnaam (e-mail, telefoonnummer of gebruikersnaam) en wachtwoord worden ingevuld.

Nieuwe gebruikers ontvangen een uitnodiging per e-mail of SMS om hun account te registreren. Gebruikers zonder e-mail of telefoonnummer kunnen zich registreren middels een registratie code.

In het registratiescherm verifiëren zij hun naam en e-mailadres/telefoonnummer of gebruikersnaam, geven aan met welk wachtwoord zij willen inloggen en kunnen zij onze Privacyverklaring en Cookiebeleid inzien. Daarnaast kunnen ze toestemming geven voor het gebruik van hun Data ter verbetering van het platform (Google Analytics). Deze toestemming is optioneel. De klant kan kiezen om deze optie niet aan te bieden.

Een voorbeeld van het registratiescherm is hier te vinden: <https://app.dialog.nl/account/register>. Je kunt geen account aanmaken via deze link. Hiervoor is een registratie code nodig die wordt meegestuurd met de uitnodigingsmail of sms.

Meer informatie over data die wordt verwerkt, is te lezen in ons Privacybeleid.

5.1.2 Single sign-on (SSO)

Het Online platform ondersteunt single sign-on (SSO) op basis van OAuth 2.0 en OpenID connect 1.0.

Wanneer er gebruik wordt gemaakt van SSO, hoeven nieuwe gebruikers geen nieuw account te registreren zoals genoemd in 'Nieuwe gebruikers'. De workflow is dan als volgt:

1. Er wordt een uitnodiging per e-mail gestuurd naar de medewerker. In plaats van een 'Registreer'-knop bevat deze mail een 'Login'-knop. Deze navigeert naar de Login van het Online platform (<https://app.dialog.nl/account/login>).
2. Op de Login-pagina vult de medewerker zijn werk e-mailadres in. Het Online platform herkent het e-mailadres als SSO e-mailadres a.d.h.v. het domein (bijv. @organisatienaam.nl).
3. Het wachtwoord-veld op de Login-pagina verdwijnt en wordt vervangen door een 'Login met je bedrijfsaccount'-knop. Deze knop navigeert naar de loginpagina van de Identity Provider.
4. Na succesvolle login met het bedrijfsaccount wordt er terug genavigeerd naar het Online platform.
5. Na de eerste succesvolle login wordt een scherm getoond met daarin de Privacyverklaring en het Cookiebeleid en toont de optie om toestemming te geven voor het gebruik van hun Data ter verbetering van het platform (Google Analytics).

Opvolgende logins gebeuren op dezelfde manier, maar dan zonder de e-mail of het Privacyverklaring/Cookiebeleid-scherm.

In de Identity Provider van de klant is het mogelijk om aanvullende beveiligingsmaatregelen in te stellen, zoals Multi Factor Authenticatie en een wachtwoordbeleid.

Meer informatie over de te ondernemen acties om SSO goed in te stellen, staan in ons Single Sign-On document. Indien jullie deze nog niet hebben ontvangen, kunnen jullie die opvragen via jullie contactpersoon of via support@dialog.nl.

5.1.3 Login

In het Online platform wordt gebruik gemaakt van JSON Web Tokens (JWT) om gebruikers bij het inloggen te onthouden.

Als een gebruiker inlogt zonder SSO gebeurt het volgende:

- De gebruiker logt in met gebruikersnaam en wachtwoord
- Er wordt een Access Token (AT) en Refresh Token (RT) gegenereerd

Als een gebruiker inlogt met SSO gebeurt het volgende:

- De gebruiker wordt doorverwezen naar de externe Identity Provider.
- Bij een succesvolle login wordt een Authorization Code (AC) gegenereerd en meegestuurd naar de browser
- De AC is 60 seconden geldig
- Bij het opstarten van de applicatie wordt AC eenmalig omgewisseld voor een AT en RT. De AC is hierna direct invalide en kan dus niet nogmaals gebruikt worden.

Voor beide login manieren geldt:

- Het AT en RT wordt opgeslagen in de browser van de gebruiker
- Het AT is 30 minuten geldig en wordt digitaal ondertekend met een HS256 algoritme.
- Het RT is 14 dagen geldig en wordt gebruikt om een nieuw AT aan te vragen wanneer deze verlopen is. Op dat moment wordt een nieuwe RT gegenereerd die weer 14 dagen geldig is. Dit heet 'Sliding Expiration'.
- Er wordt een unieke sessie opgeslagen in de productiedatabase. Deze sessie heeft een unieke ID en vervaldatum.
- Deze sessies kunnen door de gebruiker worden ingezien en beëindigd in het platform

Wanneer een gebruiker uitlogt gebeurt het volgende:

- De AT en RT worden verwijderd uit de local storage. De RT wordt geïnvalideerd en verwijderd en kan direct niet meer gebruikt worden om een nieuwe AT aan te vragen.

5.1.4 Wachtwoorden

Wachtwoordeisen

Wachtwoorden moeten minimaal uit 8 karakters en maximaal uit 128 karakters bestaan. Daarnaast mag het wachtwoord niet voorkomen in een lijst met veelgebruikte wachtwoorden.

Om gebruikers te helpen met het bedenken van een sterk wachtwoord, toont op de plek waar een wachtwoord kan worden aangemaakt een 'password strength meter'.

Wachtwoord resetten

Wanneer een gebruiker zijn wachtwoord is vergeten, kan hij een verzoek doen om zijn wachtwoord te resetten via de 'Wachtwoord vergeten?' functionaliteit. Deze functionaliteit is toegankelijk vanaf het loginscherm van het Online platform. Wanneer de gebruiker een verzoek doet, moet hij het e-mailadres van zijn account invoeren. Vanuit het bevestigingsscherm van deze functionaliteit is niet af te leiden of er een account met het ingevulde e-mailadres bestaat.

De gebruiker ontvangt een e-mail met daarin een knop met unieke link terug naar het Online platform om een nieuw wachtwoord in te voeren.

Wanneer een gebruiker te vaak probeert in te loggen met de verkeerde gebruikersnaam-wachtwoord combinatie, wordt het account voor een korte periode vergrendeld. Een gebruiker kan dan nog wel een nieuw wachtwoord aanvragen via de 'Wachtwoord vergeten?' functionaliteit. De vergrendeling wordt opgeheven na het verstrijken van de tijd of het succesvol wijzigen van het wachtwoord.

Gebruikers die proberen een wachtwoord te resetten van een account dat gemarkeerd staat als SSO account, kunnen niet hun wachtwoord resetten via het Online platform. Dit kan alleen via de Identity Provider zelf. Het Online platform attendeert gebruikers hierop als zij dit proberen te doen.

5.1.5 Sessions

Op basis van de 'Onthoud mij'- optie op de login pagina gebeurt het volgende:

- Wanneer de optie uit staat, dan:
 - De Access Token (AT) en Refresh Token (RT) worden opgeslagen in de Session Storage van de browser.
 - Wanneer de gebruiker de browser sluit, worden de AT en RT verwijderd.
 - Wanneer de gebruiker zijn browser weer opent, moet er opnieuw ingelogd worden.
- Wanneer de optie aan staat, dan:
 - De Access Token (AT) en Refresh Token (RT) worden opgeslagen in de Local Storage van de browser.
 - Na 14 dagen zonder activiteit moet de gebruiker opnieuw inloggen, omdat dan de RT is verlopen.
 - Wanneer de gebruiker de browser sluit, dan worden de AT en RT niet verwijderd.

5.1.6 Verwijderen van gebruikers

Gebruikers kunnen worden verwijderd uit het Online platform. Dit heeft de volgende gevolgen:

- De gebruiker heeft per direct geen toegang meer tot het Online platform;
- De browser sessions van de gebruiker worden geïnvalideerd;
- Persoonsgegevens van de gebruiker worden na 30 dagen automatisch verwijderd.

Alleen medewerkers van het Dialog support team kunnen deze actie ongedaan maken binnen de 30 dagen.

5.2 Afscherming en rollen

5.2.1 Afscherming per klant

Voor iedere organisatie die gebruik maakt van het Online platform wordt een aparte, afgesloten omgeving aangemaakt. Gebruikers van verschillende organisaties krijgen nooit informatie van andere organisaties, klanten of gebruikers te zien.

5.2.2 Rollen en rechten van gebruikers

Een gebruiker in het Online platform krijgt op basis van zijn of haar functie/rol binnen een organisatie toegang tot afgeschermden delen van het Online platform.

Deze rollen worden, indien dit is afgesproken met de klant, de eerste keer door Dialog toegekend op basis van instructies van de opdrachtgever. Hierna kan de organisatie zelf rollen toevoegen aan gebruikers.

De organisatie is zelf verantwoordelijk voor het zorgvuldig toekennen van rollen aan gebruikers.

Meer informatie over de verschillende rollen en rechten is te lezen op ons Help Center.

5.3 Encryptie

De database bestanden op de lokale harde schijf van de VPS worden geëncrypt door middel van EFS (Encrypting File System).

De verbinding tussen de eindgebruiker en de server is geëncrypt via HTTPS, vereist minimaal TLS 1.2 en ondersteunt alleen sterke cypher suites. De SSL certificaten worden uitgegeven door de Let's Encrypt CA (<https://letsencrypt.org/>).

De verbinding tussen de server en de database is geëncrypt.

De back-ups van de productie database worden automatisch geëncrypt.

Alle wachtwoorden worden geëncrypt door een hashing algoritme uit ASP.NET Core Identity Version 3: PBKDF2 with HMAC-SHA256, 128-bit salt, 256-bit subkey, 10000 iteration.

5.4 Foutafhandeling

Het Product Development-team doet er alles aan om fouten in het Online platform op te vangen en af te handelen. Mocht er toch een fout de eindgebruiker bereiken, dan treedt er een mechanisme in werking die de technische details van de desbetreffende fout voor de gebruiker verbergt.

Een melding van de fout wordt gedaan naar het interne error logging Slack-kanaal.

De details van de fout zijn achteraf op te halen door developers van het Product Development-team om het probleem te herleiden en op te lossen.

5.5 Browsers & devices

5.5.1 Browsers

Het Online platform ondersteunt de meeste moderne browsers. Als het gevolg van het gebruik van het TLS 1.2 protocol, ondersteunt het Online platform sommige oudere browsers niet.

Het Online platform ondersteunt de volgende browsers:

- Google Chrome 37 en hoger;
- Microsoft Edge;
- Safari 6.2 en hoger;
- Firefox 51 en hoger.

5.5.2 Tablets

Alle functionaliteit in het Online platform wordt op tablet resolutie ondersteund.

5.5.3 Mobiel

Gebruikers hoeven geen app te downloaden om gebruik te maken van het Online platform op mobiele devices. Het Online platform is als web app te benaderen via <https://app.dialog.nl>.

De belangrijkste functionaliteiten zijn hier beschikbaar voor de eindgebruiker. Alleen functionaliteiten zoals managementoverzichten en beheerschermen zijn (nog) niet toegankelijk op mobiele devices.

5.5.4 Devices ‘van de zaak’ en interne beveiligingsmaatregelen klanten

Het Online platform is een webbased online platform en maakt gebruik van automatisch verstuurd e-mails aan medewerkers. Denk hierbij aan herinneringen per e-mail om doelstellingen bij te werken of medewerkers op de hoogte te stellen van ontvangen feedback.

Wanneer een organisatie gebruik wil maken van alle functionaliteiten in het Online platform, dient er te worden gekeken naar eventueel verhinderende maatregelen die het bezoeken van het Online platform en het ontvangen van e-mails kan verhinderen. Denk hierbij aan strenge spam- en browser filters.

6. Testen en analyses

Om de beveiliging en prestaties van het Online platform te testen, voeren we regelmatig verschillende testen en analyses uit om eventuele kwetsbare plekken in kaart te brengen en daar maatregelen op te treffen.

6.1 Penetratietesten

We laten ten minste één keer per jaar een penetratietest voor het Online platform uitvoeren door een externe partij. Hierbij wordt geverifieerd dat het Online platform voldoet aan OWASP niveau 2.

Als er bevinding uit deze penetratietest komen van het niveau *medium*, *hoog*, of *kritiek* worden deze direct verbeterd. Bevindingen van het niveau *laag* worden ingepland en binnen een jaar opgelost, ter voorbereiding op de volgende penetratietest.

6.2 Loadtesting

Om er zeker van te zijn dat onze servers en het platform piekmomenten in het gebruik van het Online platform gedurende het jaar aankunnen, voeren we doorlopend load tests uit op onze server.

We simuleren met behulp van Loadster (<https://loadster.app/>) deze piekmomenten en bepalen aan de hand van de resultaten of we iets moeten verbeteren of aanpassen.

6.3 Data Protection Impact Assessment (DPIA)

De interne Data Protection Impact Assessment (DPIA) wordt jaarlijks uitgevoerd. Aan de hand van een checklist zijn de volgende analyses uitgevoerd:

- Analyse dienstverlening Dialog m.b.t. het Online platform;
- Analyse op de relevantie en categorie van verzamelde persoonsgegevens;
- Analyse interne en externe betrokken partijen m.b.t. het leveren van het Online platform;
- Analyse op de manier hoe persoonsgegevens worden verzameld;
- Analyse op de manier hoe persoonsgegevens worden verwerkt;
- Analyse op de bewaartermijnen van verzamelde persoonsgegevens;
- Analyse op de manier hoe persoonsgegevens worden beveiligd;
- Analyse op de protocollen in het geval van een datalek.

6.4 Risico analyse organisatie en informatiebeveiliging

De interne Risico analyse wordt jaarlijks uitgevoerd. Hierbij is expliciet onderscheid gemaakt tussen organisatorische en informatiebeveiliging risico's.

Aan de hand van een checklist zijn de risico's in kaart gebracht voor de volgende onderwerpen:

- Business continuity
- Leveringsproces
 - Verkoop
 - Inrichten diensten
 - Product/Beheer
- Productontwikkeling
- Ondersteunende processen
 - HRM
 - Finance
 - ICT-Beheer
 - Leveranciers beheer
 - Interne control
- Cruciale bedrijfsmiddelen
 - Medewerkers
 - Externe datacenters
 - Managementsystemen
 - Directie
- Omgeving

7. Subverwerkers

Dialog werkt samen met subverwerkers om het Online platform mogelijk te maken. Meer informatie over de manier waarop we met subverwerkers samenwerken, is te lezen in ons Privacybeleid.

8. Sourcecode

De sourcecode van het Online platform bestaat grotendeels uit maatwerk en deels uit voorgeprogrammeerde code van het applicatie framework, welke de basis vormt van de applicatie.

Het Online platform maakt in de backend gebruik van .NET 8.0 van Microsoft. Voor de frontend maken we gebruik van Angular.

De gebruikte programmeertalen voor het Online platform zijn C# in de back-end, TypeScript in de front-end.

8.1 Git

Voor het Online platform maken we gebruik van versiebeheer Git. Git is een gedistribueerd versiebeheersysteem, waarbij – in tegenstelling tot andere versiebeheer systemen – niet slechts de wijzigingen worden gedownload van de server, maar juist een complete kopie van de broncode (de ‘repository’), inclusief alle wijzigingen van alle developers.

Op deze manier is de code altijd veilig. Bij het uitvallen van één systeem kan één van de andere systemen de distributie zonder dataverlies herstellen.

8.2 Cloud

De Git repository van het Online platform wordt gehuisvest in de cloud door Github.

8.3 Toegankelijkheid

De Git repository is alleen toegankelijk voor het Product Development-team van Dialog. Er is per developer een account nodig met de bijbehorende lees- en schrijfrechten.

9. Releasebeleid

De downtime wordt voor het Online platform beperkt. Er wordt uitsluitend gereleased op 'rustige' momenten, tenzij er vanwege een kritisch technisch mankement een hotfix gedaan moet worden.

Meer informatie over ons releasebeleid is te lezen in de SLA (Service Level Agreement).

10. Product Development team

Het Product Development team van Dialog dat aan het Online platform werkt, werkt volledig volgens de SCRUM-methodiek.

Het team bestaat uit een combinatie van meerdere Developers, UX-Designers, een tester, een Scrum master en een Product Owner.

Naast het team werkt de Manager Operations, verantwoordelijk voor de Informatiebeveiliging binnen het bedrijf, nauw samen met het Product Development team om de veiligheid van het Online platform (en gegevens in het platform) te kunnen garanderen.

Tot slot heeft het team doorlopend contact met het supportteam om vragen van klanten binnen de SLA te kunnen afhandelen.