Beveiligingsbeleid

Online platform Dialog

26 november 2020 – Versie 1.6

Inhoudsopgave

1. Introductie

Dit Beveiligingsbeleid geldt voor het online platform Dialog (hierna: Dialog), gebouwd door Perflectie C.V. (hierna: Perflectie). Perflectie is geregistreerd bij de Kamer van Koophandel onder handelsnummer 58080457.

1.1 Doel

Dialog 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

Dialog 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;
- Beheerschermen om het bovenstaande als Beheerder binnen een organisatie te kunnen beheren.

1.3 Wetgeving

Als ontwikkelaars hebben we uiteraard alle maatregelen genomen om aan de wet te voldoen. Hiernaast hanteren we (het Product Development-team van Perflectie) 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 Perflectie.

1.5 Contactgegevens

Kantoor Perflectie

Ondiep-Zuidzijde 6

3551 BW, Utrecht

Nederland

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

E: support@dialog.nl

2. Server

Dialog 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 Perflectie. Medewerkers van TransIP hebben geen toegang tot de operationele zijde van Dialog.

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.

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

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

2.2 Updates

De servers worden iedere eerste zondag van de maand automatisch voorzien van de laatste updates. 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.

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

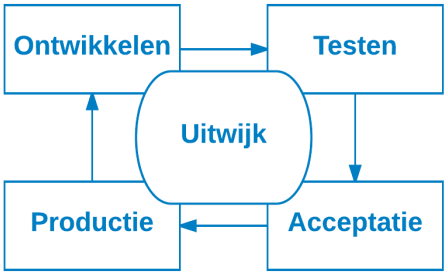
2.4 Toegankelijkheid

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

- Het datacentrum is onbereikbaar voor onbevoegden.
- De server is 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 developers van het Product Development-team hebben toegang tot de ongepseudonimseerde productiedatabase met schrijfrechten. Zij gebruiken deze database uitsluitend voor het oplossen van klantproblemen die niet op te lossen zijn met een database met fictieve data.
- Via Windows Event Logs wordt bijgehouden welke login pogingen er worden gedaan op de server.
- Gefaalde login pogingen op de server worden doorgestuurd per e-mail naar onze support inbox (support@dialog.nl). Tegelijkertijd wordt er een bericht gestuurd naar ons error logging Slack-kanaal gestuurd. Beide worden tijdens werktijden actief gemonitord.

3. OTAP (DTAP)

Bij het ontwikkelen en onderhouden van Dialog wordt gebruikt gemaakt van aparte omgevingen:



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. Development computers staan op het kantoor van Perflectie in Utrecht.

Testen: Nieuwe versies van het platform worden altijd naar de testomgeving (staging) gebracht. Hier worden alle functionaliteiten van Dialog 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.

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

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 verschillende omgevingen. De databaseversies zijn uiteraard wel hetzelfde. Hierdoor wordt de kans op bugs verkleint.

4. Database

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

4.1 Toegankelijkheid

De database server wordt beheerd door de Lead Developer.

Naast de Lead Developer hebben andere developers van het Product Development-team volledige toegang tot de database server.

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.

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 Dialog. Dit account is uitsluitend toegankelijk wanneer het goede e-mailadres en wachtwoord wordt ingevuld.

Nieuwe gebruikers ontvangen een uitnodiging per e-mail om hun account te registreren.

In het registratiescherm verifiëren zij hun naam en e-mailadres, 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.

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 activationkey nodig die wordt meegestuurd met de uitnodigingsmail.

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

5.1.2 Single sign-on (SSO)

Dialog 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 Dialog (https://app.dialog.nl/account/login).
2. Op de Login-pagina vult de medewerker zijn werk e-mailadres in. Dialog 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 Dialog.
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.

Two Factor Authenticatie is mogelijk door dit af te dwingen in de Identity Provider.

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 Dialog wordt gebruik gemaakt van cookies om gebruikers bij het inloggen te onthouden.

Na een succesvolle login, met e-mailadres en wachtwoord of via SSO, gebeurt het volgende:

- Er wordt een cookie met authenticatie, waaraan een gebruiker is gekoppeld, geplaatst in de browser van de gebruiker;
- Er wordt een unieke session opgeslagen in de productiedatabase. Deze session heeft een unieke ID en expiry date;

Bij de eerste api call die wordt uitgevoerd op de loginpagina, wordt een XSRF-TOKEN gezet om cross-site request forgery te voorkomen.

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

- Wanneer de optie uit staat, dan:
    - De browser session cookie blijft voor 2 uur staan;
    - De expiry date van de database session wordt op 2 uur na login gezet;
    - Wanneer de helft van de database session is verlopen en de gebruiker voert een actie in Dialog uit, dan wordt de database session verlengd met een uur.
    - Wanneer de gebruiker de browser sluit, dan wordt de browser session cookie verwijderd.
    - Wanneer de gebruiker zijn browser weer opent, moet hij opnieuw inloggen.
- Wanneer de optie aan staat, dan:
    - De browser session cookie blijft voor 14 dagen in de browser staan;
    - De expiry date van de database session wordt op 14 dagen na login gezet;
    - Wanneer de helft van de database session is verlopen en de gebruiker voert een actie in Dialog uit, dan wordt de database session verlengt met de helft van de totale session length.
    - Na 14 dagen moet de gebruiker opnieuw inloggen, omdat dan de session cookie is verlopen.
    - Wanneer de gebruiker de browser sluit, dan wordt de browser session cookie niet verwijderd.

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 Dialog. 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 Dialog om een nieuw wachtwoord in te voeren.

Wanneer een gebruiker te vaak probeert in te loggen met de verkeerde emailadres-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 Dialog. Dit kan alleen via de Identity Provider zelf. Dialog attendeert gebruikers hierop als zij dit proberen te doen.

5.2 Afscherming en rollen

5.2.1 Afscherming per klant

Voor iedere organisatie die gebruik maakt van Dialog 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 Dialog krijgt op basis van zijn of haar functie/rol binnen een organisatie toegang tot afgeschermde delen van Dialog.

Deze rollen worden, indien dit is afgesproken met de klant, de eerste keer door Perflectie 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.

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 Dialog 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

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

Dialog 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 Dialog wordt op tablet resolutie ondersteund.

5.5.3 Mobiel

Gebruikers hoeven geen app te downloaden om gebruik te maken van Dialog op mobiele devices. Dialog 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.

Dialog ondersteunt Android vanaf versie Android 4.4.2.

5.5.4 Devices 'van de zaak' en interne beveiligingsmaatregelen klanten

Het online platform Dialog is een web based online platform en maakt gebruik van automatisch verstuurde 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 Dialog, 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 van Dialog 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 Dialog uitvoeren door een externe partij.

De laatste penetratietest (Advanced Security Scan) is uitgevoerd door nSEC/Resilience (https://www.nsec-resilience.com/) op 20 februari 2020.

De bevindingen die uit de deze penetratietest zijn gekomen, zijn afgestemd met nSEC/Resilience. De hertest voor de penetratietest is door nSEC/Resilience uitgevoerd. Zij concluderen dat alle bevindingen zijn opgelost. Er staan geen bevindingen open.

6.2 Loadtesting

Om er zeker van te zijn dat onze servers en het platform piekmomenten in het gebruik van Dialog 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 laatste, interne Data Protection Impact Assessment (DPIA) is uitgevoerd op 1 juni 2020. Aan de hand van een checklist zijn de volgende analyses uitgevoerd:

- Analyse dienstverlening Perflectie m.b.t. het online platform Dialog;
- Analyse op de relevantie en categorie van verzamelde persoonsgegevens;
- Analyse interne en externe betrokken partijen m.b.t. het leveren van het online platform Dialog;
- 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.

De bevindingen uit de bovenstaande analyses zijn doorgenomen en de belangrijkste bevindingen zijn inmiddels opgelost.

6.4 Risico analyse organisatie en informatiebeveiliging

De laatste, interne Risico analyse is uitgevoerd op 1 juni 2020. 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

De grootste risico's uit de bovenstaande analyses zijn doorgenomen. De grootste risico's zijn inmiddels ingeperkt.

7. Subverwerkers

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

8. Sourcecode

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

Het online platform Dialog maakt in de backend gebruik van ASP.NET Core en Web API van Microsoft. Voor de frontend maken we gebruik van Angular.

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

8.1 Git

Voor het online platform Dialog maakt 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 Dialog wordt gehuisvest in de cloud door Github.

8.3 Toegankelijkheid

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

9. Releasebeleid

De downtime wordt voor het online platform Dialog 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 Perflectie dat aan Dialog 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 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.