Security Policy

December 8th, 2022 – Version 1.11

Contents

1. Introduction

This Security Policy applies to the Online platform Dialog, built by Dialog B.V. (hereinafter referred to as Dialog). Dialog is registered with the Chamber of Commerce under registration number 84510722.

1.1 Objective

The Online platform helps employees, managers and HR engage in good dialogue about objectives and development. By engaging in good dialogue, employees can make the best possible contribution to the organisation's success.

1.2 Functionalities

Amongst other things, the Online platform facilitates the following functionalities:

- Recording and updating progress on objectives at organisational, team/department and individual level;
- Requesting and giving feedback from/to colleagues and external parties;
- Completing periodic evaluations about and by an employee;
- Providing dashboards about the progress of the objectives and the use of the platform;
- Engagement measurement
- Providing management screens to manage the above as Manager within an organisation.

1.3 Legislation and regulations

As developers, needless to say we have taken any measures required to comply with the legislation and regulations. In addition, we (the Dialog Product Development team) apply our own procedures to assure the security of all recorded information and the stability of the application.

1.4 Additional Documentation

Additional documentation complementing this Security Policy:

- Privacy policy
- Privacy Statement
- Cookie Policy
- Service Level Agreement (SLA)
- Processing Agreement
- Single Sign-On document

This Security Policy may refer to the above documentation, which can be requested from Dialog at any time.

1.5 Contact Details

Dialog Office

Ondiep-Zuidzijde 6

3551 BW, Utrecht

The Netherlands

T: +31 (0)30 7600 290 (Monday to Friday, 09.00 - 17.00 hours)

E: support@dialog.nl

2. Server

The Online platform runs on a 3 TransIP Virtual Private Servers (https://www.transip.nl/). These servers are managed by Dialog's Lead Developer. TransIP employees do not have access to the operational side of the Online platform.

Dialog reserves the right to grant TransIP employees access to the servers if this is necessary for technical reasons, such as server support.

The 3 Virtual Private Servers have the following responsibilities:

1. Database server with Microsoft SQL Server 2016;
2. Application server with IIS 10 for the back-end and de front-end;
3. Hangfire (cron job) server with IIS 10 for the back-end.

2.1 Software

The servers run on Microsoft Windows Server 2019 Standard with very limited features. Virtually all software, such as IIS, is part of the Microsoft server platform. The web servers are located directly on the Internet without DMZ or WAP.

In addition, the servers are equipped with a firewall (Windows Firewall with advanced security) to block the unnecessary ports. Ports 80 and 443 are whitelisted in our firewall settings.

2.2 Updates

The production servers are automatically provided with the latest updates on the 4th Sunday of the month. Updates are preinstalled on the 2nd and 3rd Sundays of the month on our test and acceptance environments respectively. This gives us the opportunity to verify that updates do not affect the availability and security of the production servers. Critical security updates are installed within two business days.

2.3 Data Centre

The data centre is owned by The Datacenter Group in Amsterdam. The data centre has 24/7 on-site security, biometric identification and an HD CCTV network.

The virtual private servers are backed up every 4 hours and stored off-site on a different availability zone.

The data centre is ISO 9001, ISO 27001 and ISO 14001 certified, which means its quality, security and environmental management is optimally safeguarded.

2.4 Accessibility

Various measures have been taken to limit access to databases and servers.

- The data centre is inaccessible for unauthorised persons.
- The servers are only available to a limited extent via a Remote Desktop connection.
- The RDP servers can only be accessed externally by a very small list of whitelisted IP addresses.
- Only the developers of the Product Development team have read/write access to the raw production database. They only use this database to solve customer problems that cannot be resolved with a database containing fictitious data.
- Windows Event Logs track all log-in attempts being made on the server.
- Any failed login attempts on the server are forwarded by email to our support inbox (support@dialog.nl). At the same time, a message is sent to our error-logging Slack channel. Both are actively monitored during working hours.

3. DTAP

Separate environments are used for the development and maintenance of the Online platform:

Development: Developers work on new or improved functionalities in a local development environment on the developer's computer. Any bugs are also dealt with in this local environment. Development computers are located at the Dialog offices in Utrecht.

When ready, new or improved functionalities are first demonstrated to the internal test specialist and then demonstrated to the designer(s) and product owner. In both demonstrations, any improvements are immediately implemented.

As a final step, the delivered source code is reviewed by another developer and possible changes are made.

Testing: New versions of the Online platform are always transferred to the test environment (staging) first. This is where all functionalities of the Online platform are tested extensively (user acceptance tests, regression tests and automated testing). This test environment runs on a VPS with a fictitious database, which is completely separate from the production database.

Acceptance: In the acceptance environment, new functionalities are tested by implementation managers and (optionally) clients. This happens after the new release is brought to the production environment. Management sessions also take place in this environment so administrators can click around and experiment without this affecting the end user. The acceptance environment contains production data that is subject to the same security measures as those in our production environment.

Production: After extensive testing, the release candidate build is transferred to the production environment at a convenient time. This is the live environment that customers and end users work on.

More information about our release policy can be found in the SLA (Service Level Agreement) document.

There is no automatic synchronisation between the four different environments. They are separate, independent environments.

No data is exchanged between the development and test environments on the one hand, and the production and acceptation environment on the other. The database versions are, of course, the same, thus reducing the risk of bugs.

4. Database

The Online platform uses an instance of SQL Server 2016. The database server is not used for any other applications and/or purposes.

4.1 Accessibility

The database server is managed by the Lead Developer.

In addition to the Lead Developer, other developers in the Product Development team have full access to the database server.

4.2 Backup

A backup is made of the Production Database every day. This happens at night and is fully automatic.

The backups of the Production Database are stored on Cloud Storage hosted by Amazon Web Services (AWS). Before these backups are stored at AWS, they are encrypted using AES-256 encryption. Back-ups are not anonymised.

The servers where these backups are stored are located in Frankfurt, Germany. The stored backups do not leave the EU.

Backups are automatically deleted from the Cloud Storage service 60 days after creation.

5. Application

5.1 Accounts, Login, Passwords and Single Sign-on

5.1.1 New Users

Each user has their own account in the Online platform. This account is only accessible when the correct username (email address, phone number or username) and password are entered.

New users receive an invitation by email or SMS to register their account. Users without email or telephone number can register with a registration code.

In the registration screen they verify their name and e-mail address/telephone number or username, indicate with which password they want to log in and they can view our Privacy Statement and Cookie Policy. In addition, they can give permission for the use of their Data to improve the platform (Google Analytics). This permission is optional.

An example of the registration page can be found here: https://app.dialog.nl/account/register. You cannot create an account via this link as this requires an activation key, which will be sent along with the invitation email or SMS.

More information about the data that will be processed can be found in our Privacy Policy.

5.1.2 Single Sign-on (SSO)

The Online platform supports single sign-on (SSO) based on OAuth 2.0 and OpenID connect 1.0.

When SSO is used, new users do not need to register a new account as mentioned in ‘New users’. In that case, the workflow is as follows:

1. An invitation is sent to the employee by email. Instead of a ‘Register’ button, this mail contains a ‘Login’ button. This navigates to Dialog’s Login (https://app.dialog.nl/account/login).
2. On the login page, the employee enters his work email address. The Online platform recognises the email address as an SSO email address by checking the domain (for example @organisation.nl).
3. The password field on the Login page disappears and is replaced with a ‘Log in with your company account’ button. This button navigates to the Identity Provider’s login page.
4. After successful login with the company account, the user is directed back to the Online platform.
5. After the first successful login, a screen will be displayed containing the Privacy Statement and Cookie Policy, also showing the option to consent to the use of their Data to improve the platform (Google Analytics).

Subsequent logins are performed in the same way, but without the email or the Privacy Statement/Cookie Policy screen.

Two-factor Authentication is possible by enforcing this in the Identity Provider.

More information about the actions to be taken to correctly set up SSO can be found in our Single Sign-On document. If you have not yet received it, you can request this via your contact person or via support@dialog.nl.

5.1.3 Login

The Online platform uses cookies to remember users when they log in.

After a successful login with email address and password or via SSO, please note the following:

- An authentication cookie to which a user is linked is placed in the user's browser.
- A unique session is stored in the production database. This session has a unique ID and expiry date.

During the first api call executed on the login page, an XSRF-TOKEN is set to prevent cross-site request forgery.

5.1.4 Passwords

Password requirements

Passwords must consist of at least 8 characters and a maximum of 128 characters. In addition, the password may not appear in a list of frequently used passwords.

To help users come up with a strong password, the page on which a password can be created shows a password strength meter.

Password reset

If a user has forgotten his password, he can ask for a reset using the 'Forgot password?' functionality. This functionality can be accessed from the login screen of the Online platform. When making a request, the user must enter the email address of his account. The confirmation screen of this functionality does not indicate whether there is an account with the entered email address.

The user will receive an email containing a button with a unique link back to the Online platform to enter a new password.

When a user tries too often to log in with the wrong email address password combination, the account is locked for a short period of time. A user can still request a new password via the 'Forgot password?' functionality, however. The account is unlocked once the time has expired or the password has been changed successfully.

Users who try to reset a password from an account marked as SSO account cannot reset their password via the Online platform. This can only be done via the Identity Provider itself. The Online platform alerts users to this when they try to do so.

5.1.5 Sessions

Based on the ‘Content Me’ option on the login page, the following happens:

- If the option is switched off:
    - The browser session cookie is stored for 2 hours.
    - The expiry date of the database session is set to 2 hours after login.
    - If half of the database session has expired and the user performs an action in the Online platform, the database session is extended by one hour.
    - When the user closes the browser, the browser session cookie is deleted.
    - When the user opens his browser again, he must log in again.
- If the option is switched on:
    - The browser session cookie is stored in the browser for 14 days.
    - The expiry date of the database session is set to 14 days after login.
    - If half of the database session has expired and the user performs an action in the Online platform, the database session is extended by half of the total session length.
    - After 14 days, the user must log in again because the session cookie has expired.
    - When the user closes the browser, the browser session cookie is not deleted.

5.1.6 Deleting users

Users can be removed from the Online platform. This has the following consequences:

- The user will no longer have access to the Online platform with immediate effect;
- The user's browser sessions are invalidated;
- Personal data of the user is automatically deleted after 30 days.

Only employees of the Dialog support team can undo this action within 30 days.

5.2 Segregation and Roles

5.2.1 Segregation of each Customer

A separate, closed environment is created for each organisation that uses the Online platform. Users of different organisations never get to see information related to other organisations, customers or users.

5.2.2 Roles and User Permissions/Rights

Someone using the Online platform will be given access to protected parts of the Online platform based on his or her function/roles within the organisation.

If this has been agreed with the client, these roles are assigned by Dialog the first time based on instructions from the client. After this, the organisation itself can assign roles to users.

The organisation itself is responsible for carefully assigning roles to users.

More information about the various roles and permissions/rights can be found at our Help Centre.

5.3 Encryption

The database files on the local VPS hard disk are encrypted using EFS (Encrypting File System).

The connection between the end user and the server is encrypted via https, requires at least TLS 1.2 and only supports strong cypher suites. The SSL certificates are issued by the Let's Encrypt CA (https://letsencrypt.org/).

The connection between the server and the database is encrypted.

The backups of the production database are encrypted automatically.

All passwords are encrypted using a hashing algorithm from ASP.NET Core Identity Version 3: PBKDF2 with HMAC-SHA256, 128-bit salt, 256-bit subkey, 10000 iteration.

5.4 Error Handling

The Product Development team does everything in its power to detect and deal with errors in the Online platform. Should an error still reach the end user, however, a mechanism will take effect that hides the technical details of the relevant error from the user.

The error-logging Slack channel is notified of the internal error.

The details of the error can be retrieved afterwards by developers of the Product Development team so they can trace and resolve the problem.

5.5 Browsers & Devices

5.5.1 Browsers

The Online platform supports most modern browsers. Due to the use of the TLS 1.2 protocol, the Online Platform does not support some older browsers.

The Online platform supports the following browsers:

- Google Chrome 37 and above
- Microsoft Edge
- Safari 6.2 and above
- Firefox 51 and above

5.5.2 Tablets

All functionality in the Online platform are supported in tablet resolution.

5.5.3 Mobile

Users do not need to download an app to use Online platform on mobile devices. The Online platform can be accessed as a web app via https://app.dialog.nl.

The main functionalities are available for the end user here. Only functionalities such as management overviews and management screens are not (yet) accessible on mobile devices.

The Online platform supports Android version Android 4.4.2 and above.

5.5.4 'Company' devices and internal customer security measures

The Online platform is a web-based online platform that uses emails sent automatically to employees. Examples include reminders by email to update objectives or to inform employees of any feedback received.

If an organisation wishes to make use of all functionalities of the Online platform, it is important to check any measures that may prevent access to the Online platform and receiving email. This includes strict spam and browser filters.

6. Testing and Analyses

To test the security of the Online platform, we regularly perform various tests and analyses to identify any vulnerable locations and resolve any issues.

6.1 Penetration Tests

We ask an external party to perform a penetration test for the Online platform at least once a year.

The latest penetration test (Advanced Security Scan) was performed by nSEC/Resilience (https://www.nsec-resilience.com/) in February 2022. It has been verified that the Online platform complies with OWASP level 2.

The findings from this penetration test were discussed with nSEC/Resilience. The retest was performed by nSEC/Resilience. They concluded that the platform is secure and found no outstanding findings of severity medium and high.

6.2 Load Testing

We continuously conduct load tests on our server to ensure our servers and the Online platform can handle peak use periods during the year.

We simulate these peak periods using Loadster (https://loadster.app/)and the results determine whether we need to improve or adjust anything.

6.3 Data Protection Impact Assessment (DPIA)

The latest Internal Data Protection Impact Assessment (DPIA) was performed on 1 June 2022. Based on a checklist, the following analyses were performed:

- Analysis of Dialog services regarding the Online platform.
- Analysis of the relevance and category of personal data collected.
- Analysis of internal and external stakeholders regarding the supply of the Online platform.
- Analysis of how personal data is collected.
- Analysis of how personal data is processed.
- Analysis of the retention periods of personal data that has been collected.
- Analysis of how personal data is secured and safeguarded.
- Analysis of the protocols in the event of a data breach.

The findings from the above analyses were examined and the main findings have now been dealt with.

6.4 Organisational Risk Analysis and Information Security

The latest internal Risk Analysis was performed on 1 June 2022. In the analysis, an explicit distinction was made between organisational and information security risks.

Based on a checklist, risks were identified for the following topics:

- Business continuity
- Delivery process
    - Sales
    - Setting up services
    - Product/Management
- Product development
- Supporting processes
    - HRM
    - Finance
    - ICT Management
    - Supplier management
    - Internal control
- Crucial assets
    - Employees
    - External data centres
    - Management systems
    - Management Board
- Environment

The main risks found during the analyses have been investigated. They have now been mitigated.

7. Sub-processors

Dialog works with sub-processors to facilitate the Online platform. More information about how we work with sub-processors can be found in our Privacy Policy.

8. Source Code

The Online platform´s source code largely consists of tailored and partly of pre-programmed code of the application framework that forms the basis of the Dialog application.

The Online platform uses .NET 5.0 from Microsoft for the backend. We use Angular for the front end.

The Online platform uses programming languages C# for the backend and TypeScript for the frontend.

8.1 Git

For the Online platform, Dialogue uses Git version control. Git is a distributed version control system, which, unlike other version control systems, doesn't only download the changes from the server, but a complete copy of the source code (the 'repository'), including all developer modifications.

This means the code is always secure. If one system fails, one of the other systems can restore the distribution without loss of data.

8.2 Cloud

Github stores the Online platform´s Git repository in the Cloud.

8.3 Accessibility

The Git repository can only be accessed by the Dialog Product Development team. Each developer needs an account with the correct read/write permissions.

9. Release Policy

Downtime for the Online platform is limited. Releases only take place at ‘quiet’ times, unless a hotfix needs to be performed to fix a critical technical fault.

More information about our release policy can be found in the SLA (Service Level Agreement).

10. Product Development Team

The Dialog Product Development team that works on the Online platform works according to the SCRUM method.

The team consists of a combination of multiple Developers, UX Designers, a tester, a Scrum master and a Product Owner.

In addition to the team, the Operations Manager, responsible for Information Security within the company, works closely with the Product Development team to ensure the security of the platform (and the data on the platform).

And finally, the team is in continuous contact with the support team so it can deal with questions from customers within the framework of the SLA.