**BIJLAGE 2**

**Benodigde technische documentatie**

Jullie oplossing wordt in het kader van de publieke beproeving op de aspecten betrouwbaarheid en veiligheid getest. Dit doen we om tot een goed geïnformeerde en afgewogen keuze te komen.

Om dit te doen worden de volgende tests uitgevoerd:
1. Privacy check, op basis van de door u aangeleverde documenten
2. Securiy test
3. Basis broncode-review

De security test wordt op jullie eigen testomgeving uitgevoerd. Het is van belang dat het een geïsoleerde omgeving is en indien nodig snel hersteld kan worden. Deze testen worden uitgevoerd door ons geselecteerde onafhankelijke experts van KPMG. Zij hebben hiervoor op IP-adresniveau toegang tot uw testomgeving nodig.

Let op! De security test kan pas aanvangen nadat zowel door u als KPMG een geheimhoudingsverklaring is getekend door zowel u als KPMG. Voorafgaand aan de test zal daarvoor gelegenheid zijn. Ter informatie treft u de geheimhoudingsverklaring aan in **bijlage 2A**.

We verzoeken u om de volgende informatie voor vrijdag (17-04-2020) 09.00 uur aan te leveren bij 5.1.2e 5.1.2e @kpmg.nl / 5.1.2e ) met de door u getekende Letter of Authorisation - **bijlage 2B**. Waarin u verklaart dat KPMG toegang krijgt tot uw broncode en de testen mag uitvoeren.

- Technisch contactpersoon bij uw organisatie
- Een beschrijving van jullie testomgeving (front-end als back-end)
- IP-Adres van de testomgeving
- Inloggegevens
- Alle technische documentatie
- Releasenotes
- Technisch ontwerp
- Installatie handleiding (front-end als back-end)
- API
- Ondertekening letter of authorisations

Wat betreft de basis broncode-review verzoeken wij u om de broncode beschikbaar te stellen.

In de tabellen hieronder treft u aanvullende informatie over de aanpak van de testen en de benodigde informatie hiervoor.

Wat wordt er gedaan met de testresultaten?
De testresultaten kunt u eventueel gebruiken om uw software dit weekend te verbeteren.

De uitkomsten van de security test en de basis broncode-review worden hiernaast gebruikt bij de bespreking met expertpanels op zaterdag.

## BENODIGDE DOCUMENTATIE

| Type test | Benodigde documentatie | Required documentation |
|---|---|---|
| **Source Review** | • Broncode (front- en back-end)<br>• Gebruikte externe librairies (wat is nodig om eventueel te compileren)<br>• Technische documentatie (inclusief eventueel benodigde externe componenten als databases)<br>• Functionele beschrijving<br>• Release notes<br>• API/Interface beschrijving | • Source code (front- and back-end)<br>• Required external librairies and components (like databases, operating systems) including version<br>• Technical documentation<br>• Functional description<br>• Release notes<br>• API/Interface definition |
| **Security test** | • Uitgebreide technische documentatie van het IT-landschap, inclusief netwerktopologie, IP-adressen, gebruikte poorten, en communicatiestroomlijnen.<br>• Technische ontwerpdocumentatie van de app en de backend, inclusief functionaliteitbeschrijvingen zoals inter-app communicatie, local storage, interfaces (inclusief bluetooth, NFC, internet, etc.), services, en permissies.<br>• Instellingen van de app en backend-omgeving op basis van ontwerpdocumentatie.<br>• Security requirements van de app, de communicatie tussen app en backend, en van de backend zelf.<br>• Een ondertekende vrijwaringsverklaring (ookwel Letter of Authorisation of LoA genoemd).<br>• Whitelisting van ons IP-adres om de backend te kunnen benaderen (indien van toepassing). Onze IP-range is 217.100.97.152/29. | • Extensive technical documentation of the IT landscape, including network topology, IP addresses, ports used, and communication lines.<br>• Technical design documentation of the app and the backend, including functionality descriptions such as inter-app communication, local storage, interfaces (including bluetooth, NFC, internet, etc.), services, and permissions.<br>• Configuration of the app and the backend according to technical design.<br>• Security requirements of the app, the communication between app and backend, and of the backend itself.<br>• A signed letter of authorisation (LOA).<br>• Whitelisting of our IP address to access the backend (if applicable). Our IP range is 217.100.97.152/29. |

## AANPAK

| Type test | Aanpak | Approach |
|---|---|---|
| **Source Review** | In het broncode onderzoek met nadruk op de betrouwbaarheid zullen we de opgeleverde broncode van zowel de front- en (indien van toepassing) back end applicatie inspecteren. Met behulp van automatische tooling zullen wel veel gebruikte softwaremetrieken zoals Lines of Code (LOC), Complexiteit en Duplicatie bepalen. Vanuit beschikbare tooling voor de specifiek ontwikkelplatform zullen we zo mogelijk bevindingen krijgen op Betrouwbaarheid, Beveiligbaarheid en Onderhoudbaarheid. Vanuit de focus van dit onderzoek zullen we de bevindingen op Betrouwbaarheid en Beveiligbaarheid handmatig nalopen.<br><br>We zullen verder controleren of de software afhankelijk is van externe bibliotheken; of deze bibliotheken courant zijn en of er voor deze bibliotheken bevindingen op het gebied van Betrouwbaarheid, Beveiligbaarheid bekend zijn.<br>Tenslotte, zullen we controleren of the broncode in lijn is met onze verwachtingen die gebaseerd zijn op de technische en functionele documentatie en of er data uitgangen of interface zijn (inclusief logbestanden) behalve die zijn gespecificeerd We zullen daarbij aandacht geven of de beschreven privacy mechanismen zijn geïmplementeerd. Als er crypto grafische algoritmen worden gebruikt (binnen de geleverde software) dan zullen nalopen of deze veel gebruikt getest en actueel zijn.<br><br>Een broncode onderzoek geeft een indruk of de software geschikt is voor haar taken. Een functioneel testprogramma is noodzakelijk om te bepalen of het systeem geschikt is voor gebruik en niet (te veel) bugs bevat. | For the source code scan with focus on reliability we will inspect the presented source code of both the front- and (if applicable) back-end application. With the aim of automated tooling we will determine common software metrics like Lines of Code (LOC), Complexity and Duplication. Based on the availability of tooling for the specific software platforms we will get findings on Reliability, Security and Maintainability. Seen the focus of this assignment we will verify the findings on Reliability and Security by hand. We will furthermore check whether the software depends on external libraries; if these libraries are current and maintained and if there are known Reliability and Security findings in the libraries.<br><br>Finally, we will check whether the source code is in line with our expectations based on the technical and functional documentation and if there no data outputs or interfaces (including logfiles) except those specified. We specifically will look if described privacy mechanisms are implemented. If cryptographic algorithms are used (inside the presented source code) we will check whether those are common, tested and current.<br><br>This source code review will give an overall impression whether the software is suitable to execute it tasks. A functional testing program is required to determine whether the system is fit for use and does not contain (to many) bugs. |
| **Security test** | Wij voeren een initiële penetratietest uit op de COVID-19 app, de bijbehorende backend en de communicatie tussen de app en de backend volgens het "white box"-principe. Dit houdt onder andere in dat wij voorafgaand uitgebreide toegang krijgen tot documentatie, systeemconfiguratie, en andere opgevraagde informatie. Op deze manier kunnen wij zeer efficiënt te werk gaan. Tegelijkertijd krijgen we een beeld over wat een aanvaller mogelijk zou | We will perform a an initial exploratory penetration test on the COVID-19 app, the associated backend and the communication between the app and the backend, applying the "white box" principle. This means that we obtain extensive access to documentation, system configuration, other requested information, etc. in advance. In this way we can work very efficiently. We can get an initial idea what an attacker could possibly do if |

| | | |
|---|---|---|
| | kunnen doen indien deze informatie niet beschikbaar is voor hem. Op basis van deze informatie stellen wij vast welke scenario's het meest relevant zijn om te testen tijdens de penetratietest. Op basis van deze scenario's doorlopen wij de volgende drie fases van onze penetratietest:<br><br>1 Identificatiescanfase: verschillende identificatie scans uitvoeren op de backend-omgeving. Met deze stap verkrijgen wij gedetailleerde informatie over welke poorten en services actief zijn;<br><br>2 Kwetsbaarhedenscan: wij gebruiken efficiënte tools die bekende kwetsbaarheden identificeren in systemen. Deze tools en scans worden toegepast op de backend-omgeving. Ook wordt er handmatig gescand voor eventuele kwetsbaarheden, zowel op infrastructuur- als applicatie-niveau die ingaan op de app, de backend en de communicatie tussen de app en de backend;<br><br>3 Uitbuiting: wij voeren handmatige controles uit om vast te stellen of de in de vorige stappen verkregen kwetsbaarheden daadwerkelijk aanwezig zijn (de zogenaamde "false positive"-verificatie). Wij testen verder handmatig op kwetsbaarheden en buiten deze uit waar mogelijk. Op deze manier kunnen wij de impact bepalen van de kwetsbaarheden. | this information is not available to him. Based on this information, we will determine which scenarios are most relevant to test during the penetration test. Based on these scenarios, we go through the following three phases of our penetration test:<br><br>1 Identification scan phase: perform various identification scans on the backend environment. With this step we obtain detailed information about which ports and services are active.<br><br>2 Vulnerability scan: we use tools that efficiently identify known vulnerabilities. We will also perform manual scanning for possible vulnerabilities, both at infrastructure and application level, focussed on the app, the backend and the communication between the app and the backend.<br><br>3 Exploitation: We will perform manual checks to determine whether the vulnerabilities obtained in the previous steps are present in practice (the so-called "false positive" verification). We will also manually test the system for vulnerabilities and exploit them where possible. In this way we can determine the impact of the vulnerabilities. |