



Statement of Work
PENTEST SNPG WEBAPPLICATIE
voor
RIVM

5.1.2e

20121092v1.0-RIVM-Pentest SNPG Webapp
Versie 1.0
29-12-2020

VERTROUWELIJK

VERTROUWELIJK



SAMENVATTING

Binnenkort starten in Nederland de inentingen tegen het Coronavirus (COVID-19). Het RIVM speelt hierin een centrale rol. De webapplicatie SNPG wordt gebruikt voor het bestellen van de vaccins door huisartsen en artsen van zorgorganisaties en later in het jaar voor de declaraties van huisartsen en de opgaven van de artsen van zorgorganisaties. Het is belangrijk dat alle bestelgegevens veilig worden verwerkt en opgeslagen.

5.1.2e heeft daarom aan 5.1.2e van Secura gevraagd om een opdrachtbevestiging te maken voor het op korte termijn uitvoeren van een security assessment op de SNPG webapplicatie, de API koppelingen en onderliggende infrastructuur. Deze opdracht is urgent en moet op zeer korte termijn uitgevoerd worden.

VERTROUWELIJK



Project overzicht	
Projectnaam:	Pentest SNPG Webapp
Doel:	Secura zal de effectiviteit van de geïmplementeerde beveiligingsmaatregelen testen, kwetsbaarheden identificeren en heldere adviezen geven ter verbetering van de SNPG-applicatie.
Scope:	In scope is de SNPG webapplicatie (acceptatie.influenzavaccinatie.nl) en de daaraan gekoppelde API's / endpoints, inclusief onderliggende infrastructuur. Daarnaast onderzoeken wij de broncode als onderdeel van het onderzoek. Een heronderzoek van de bevindingen is ook in scope
Onderzoeksmethode:	Crystal Box application test + Black Box infrastructuurtest op onderliggende infrastructuur
Bijzonderheden:	Deze opdracht is urgent en moet op korte termijn uitgevoerd worden. Secura en het RIVM hebben daarom besloten om op een praktisch manier met elkaar deze opdracht uit te voeren. Dit Statement of Work dient als opdracht bevestiging.
Deliverable:	Bij hoge/kritieke bevindingen zullen wij deze meteen (telefonisch) doorgeven aan de gewenste contactpersonen. Na het beveiligingsonderzoek krijgt u een schriftelijk rapport met daarin: <ul style="list-style-type: none"> Een managementsamenvatting met daarin de scope van het uitgevoerde onderzoek, alle belangrijke bevindingen, risico's en aanbevelingen om de risico's tegen te gaan (mitigatie). Technische hoofdstukken met de bevindingen en beschrijvingen van de uitgevoerde tests met alle benodigde informatie om de resultaten te kunnen reproduceren. rapport presentatie dmv een video-conference call.
Planning & Uitvoering:	Secura zal op verzoek het onderzoek direct opstarten. Het onderzoek heeft inclusief voorbereiding, projectmanagement, uitvoering, rapportage en kwaliteitscontrole een omvang van 15 mandagen; Het RIVM heeft gevraagd aan Secura voor 31 december het onderzoek af te ronden: dit is omwille van de kwaliteit en de beperkte beschikbaarheid van mensen niet mogelijk. De gemaakte afspraak voor de deadline is woensdag 6 januari 2021 om 17:00u voor oplevering van het rapport, waarna we aansluitend om 17:15 het rapport zullen presenteren. Om deze deadlines te kunnen halen is het een voorwaarde dat we volledige medewerking krijgen van het RIVM en dat we vandaag (29/12/2020) kunnen starten met het onderzoek.
Fixed Prijs (vaste prijs)	5.1.2b excl. BTW inclusief heronderzoek

Als u naar aanleiding van dit voorstel vragen of aanvullingen heeft, neem dan gerust contact met mij op. In alle gevallen zien we uit naar uw reactie en het vervolg op dit voorstel.

VERTROUWELIJK



Met vriendelijke groet,
Namens Secura,

5.1.2e

5.1.2e

5.1.2e

VERTROUWELIJK



BEGROTING

Aan de hand van de informatie uit de intake heeft een securityconsultant van Secura een inschatting gemaakt van de benodigde tijd voor het project. Hieronder vindt u de daarbij behorende begroting.

Security Assessment	Totaal
Pentest SNPG Webapplicatie inclusief: <ul style="list-style-type: none"> • Voorbereiding • Rapportage en toelichting • Projectmanagement en kwaliteitscontrole 	5.1.2b
Heronderzoek	5.1.2b
Totaal (vaste prijs)	5.1.2b

Bovenstaande begroting is gebaseerd op de kennis en ervaring van Secura en de beschikbaar gestelde informatie door RIVM. Wanneer (bij een vaste prijs voorstel) door onvoorziene omstandigheden significante delen van de scope niet onderzocht kunnen worden, zal Secura hierover met RIVM overleggen.

VRIJWARING

Met het ondertekenen van deze SoW of het verstrekken van een inkooporder verstrekt RIVM toestemming aan Secura tot het uitvoeren van dit onderzoek. Tevens vrijwaart RIVM Secura voor mogelijke schadeclaims – inclusief claims van derden – voor directe en indirecte schade als gevolg van het uitvoeren van deze opdracht.

Indien de te onderzoeken systemen geen eigendom zijn van RIVM, dient de eigenaar van de systemen ook toestemming voor uitvoering van het onderzoek en vrijwaring te geven. RIVM is verantwoordelijk voor het verkrijgen van de toestemming en vrijwaring van de eigenaar van het systeem en van eventuele derden.

VERTROUWELIJK



OVEREENKOMST EN ONDERTEKENING

Deze offerte is 30 dagen geldig vanaf de datum van ondertekening door Secura. Alle genoemde prijzen zijn in Euro, inclusief reiskosten binnen Nederland, exclusief B.T.W. en gebaseerd op het werken tijdens normale kantoortijden (tussen 08:00u-18:00u). Bij dit aanbod zijn de kosten voor het gebruik van tooling en kantoorkosten inbegrepen.

Secura factureert RIVM na het opleveren van het (concept)rapport. De betalingstermijn is 30 dagen na factuurdatum.

Keuze	Beschrijving
<input checked="" type="checkbox"/>	Beveiligingsonderzoek zoals beschreven, inclusief heronderzoek

Op deze overeenkomst zijn de ARVODI 2018 voorwaarden van toepassing.

Voor akkoord:

RIVM	Secura B.V.
Datum:	Datum: 29-12-2020
Naam:	Naam: 5.1.2e
Functie:	Functie: 5.1.2e
Handtekening:	Handtekening: 5.1.2e
20121092v1.0-RIVM-Pentest SNPG Webapp 29-12-2020	