To: (10)(2e))[(10)(2e) @minvws.nl]
Cc: (10)(2e) (10)(2e) [(10)(2e)]; (10)(2e))[(10)(2e) @minvws.nl]
From: (10)(2e) (10)(2e)
Sent: Wed 7/22/2020 9:04:53 AM
Subject: Re: Procedureel assessment
Received: Wed 7/22/2020 9:04:58 AM

Ja akkoord!

On 22 Jul 2020, at 10:59, (10)(2e)) < (10)(2e) @minvws.nl> wrote:

Hi (10)(2e) ook ervanuit gaand dat (10)(2e) deze kent akkoord bij deze !

Grt (10)(2e)

Van: (10)(2e) (10)(2e) < (10)(2e) >
Verzonden: dinsdag 21 juli 2020 21:59
Aan: (10)(2e)) < (10)(2e) @minvws.nl>
Onderwerp: Procedureel assessment

Hoi (10)(2e)

Voor het controleren van de backend moet ik een assessment bestellen. Dat moet via inkoop in HIS. De inkoopwaarde is (10)(2b) euro ex. BTW. GRAAG AKKOORD.

Hieronder de uitvraag, zoals ik hem heb opgesteld:

Voor het Ministerie van VWS ben ik op zoek naar een assessment op de backend-omgeving van CoronaMelder (de notificatiie app) . Deze oplossing zal worden gehost door het CIBG met ondersteuning van KPN.

De backend bestaat uit:

1. Een omgeving om sleutels van mogelijk COVID-19 besmette personen te ontvangen.
2. Een omgeving voor het vrijgeven van de sleutels bij het positief testen op COVID-19 door de GGD'en via een portaal.
3. Een omgeving om vrijgegeven sleutels tijdelijk publiekelijk beschikbaar stellen via een CDN.
4. Een bewakingsdienst (een zogenaamd Security Operations Center, kortweg SOC).

Het assessment heeft tot doel zekerheid te verkrijgen op een aantal punten:

1. Het hebben genomen van relevante beveiligingsmaatregelen in de datacenter, die zich verhouden tot de Baseline Informatiebeveiliging Overheid op niveau BBN: 2 of een vergelijkbare norm, waardoor er matching kan worden gemaakt.
2. Verificatie van de instellingen conform de gemaakte afspraken en beloftes in de DPIA.
3. Inventarisatie van de aanwezige certificering, validatie van de certificaten.
4. Beschikbaarheid van relevante DPIA's rond SOC, datacenter en het beheersbaar hebben van de privacyrisico's.
5. Voldoen aan de NIB-richtlijn en Cyber Security Act normeringen (voor zover van toepassing uiteraard).

Voor het assessment is relevante kennis van belang en uiteraard beschikbaarheid:

1. In aanloop naar het uitvoeren van het assessment is er regelmatig overleg om daarmee zeker te stellen dat de juiste informatie beschikbaar is voor de daadwerkelijk uitvoeren van de assessment.
2. Beschikbaarheid voor verificatiebezoeken in de week van 10 augustus 2020 en kunt uiterlijk 16 augustus 2020 uw verslag aanleveren.
3. U beschikt over accreditatie van ENISA en/of een national body (in Nederland het NCSC) voor de Cyber Security Act en/of standaarden rond de NIB-richtlijn
4. Expertise op op eHealth en medische applications.
5. Bekend met het uitvoeren van assessments aan het zorgdomein gespecificeerd.
6. Omdat dit een zeer gevoelig traject betreft zal de rapportage zal openbaar worden gemaakt.
7. De rapportage wordt onder een creative commons licentie beschikbaar gesteld.
8. De rapportage moet duidelijk maken hoe is gewerkt en u schrijft zoveel mogelijk reproduceerbaar. Hierdoor is verificatie mogelijk.
9. Bereidheid tot mondelinge of schriftelijke tussentijdse verslaglegging.
10. Aantoonbare ervaring met validatie en audits op medische applicaties kunnen toevoegen alsmede ervaring met ontwikkeltrajecten.

--

(10)(2e) 1 (10)(2e)

06- (10)(2e)

(10)(2e)