[redacted]
Universiteit Twente
EEMCS-DACS
Zilverling 5055
Postbus 217
7500 AE Enschede

[redacted]

26 juli 2023

Gemeente Hillegom
Postbus 32
2180 AA HILLEGOM

Beste gemeente Hillegom,

In het kader van een onderzoek van de Universiteit Twente naar hoe met responsible disclosure-verzoeken wordt omgegaan zou ik graag van u de volgende informatie ontvangen op basis van de Wet Open Overheid (WOO):

1. De vigerende beleidsdocumenten aangaande het omgaan met meldingen van derde partijen over beveiligingslekken (ook bekend als het "responsible disclosure"- of "coordinated vulnerability disclosure"-beleid), inclusief de beleidsdocumenten aangaande de gegevens die bij een "responsible disclosure"-melding worden opgeslagen over de melding en melder, alsmede alle voorgaande iteraties, inclusief conceptversies, van deze beleidsdocumenten vanaf het vigerende beleidsdocument op 1 juli 2022;
2. Alle communicatie, notities, besluiten, informatie en beslissingen, en andere stukken die betrekking hebben op de totstandkoming van het huidige beleid of eerdere versies van dit beleid, inclusief alle overwegingen die uiteindelijk niet in beleidsdocumenten zijn opgenomen, vanaf het vigerende beleidsdocument op 1 juli 2022, alsmede toekomstige versies van dit beleid;
3. Alle evaluaties, zowel intern als extern, op alle iteraties van het beleid, inclusief conceptversies van beleidsdocumenten die nooit gepubliceerd zijn, vanaf het vigerende beleid op 1 juli 2022, zowel in het verleden, heden, als toekomst;
4. Bij het ontbreken van huidig beleid, alle communicatie, notities, besluiten, informatie en beslissingen over het (mogelijk) vormen van toekomstig beleid.

Graag zou ik deze informatie digitaal en/of schriftelijk ontvangen. Ik word graag op de hoogte gehouden van de voortgang.

De Universiteit Twente, en dus ook dit onderzoek, houdt zich aan de Nederlandse gedragscode wetenschappelijke integriteit[1], zoals gepubliceerd door de NWO.

Mochten er vragen zijn, neem dan gerust contact op. De contactgegevens staan bovenaan deze brief.

Alvast bedankt.

Met vriendelijke groeten,

[redacted]

[redacted]

[1]https://www.nwo.nl/nederlandse-gedragscode-wetenschappelijke-integriteit

Gemeente Hillegom

Postbus 32
2180 AA Hillegom
T 14 0252
E gemeente@hillegom.nl

Universiteit Twente
T.a.v. [redacted]
Postbus 217
7500 AE Enschede

Uw kenmerk:
Ons kenmerk: Z-23-326193
Verzenddatum: 2 augustus 2023
Onderwerp: Reactie op Woo-verzoek
Behandelaar: [redacted]

Geachte heer [redacted]

Op 26 juli 2023 hebben wij uw verzoek gedateerd op 26 juli 2023 via de e-mail ontvangen. Op 27 juli 2023 ontvingen wij uw verzoek via de post. Uw verzoek is in ons systeem geregistreerd onder nummer Z-23-326193.

Verzoek om informatie
U verzoekt om, in het kader van een onderzoek van de Universiteit Twente naar hoe met responsible disclosure verzoeken wordt omgegaan, documenten openbaar te maken. U doet hierbij een beroep op de Wet open overheid (Woo).

Inventarisatie documenten
Op basis van uw verzoek heb ik gezocht in de digitale archiefsystemen en e-mail inboxen van betrokken medewerkers.

Er zijn documenten aangetroffen
Bij deze inventarisatie zijn de volgende documenten aangetroffen:

1. 20211109 e-mail Re: kwetsbaarheden melden
2. 20211110 e-mail RE: kwetsbaarheden melden HLTsamen
3. 20211110 e-mail RE: kwetsbaarheden melden

Al openbare documenten
De Woo is niet van toepassing op documenten die al openbaar zijn. Het beleid van de gemeente Hillegom is gepubliceerd op de gemeentelijke website. U kunt dit vinden via de link Gemeente Hillegom: Kwetsbaarheden melden .
De CISO heeft desgevraagd aangegeven dat er geen andere versies van het beleidsstuk meer zijn. Het document dat op de website staat is het vigerend beleid.

Besluit
Openbaar met uitzondering van persoonsgegevens
Ik besluit bovengenoemde drie documenten openbaar te maken, met uitzondering van de persoonsgegevens, die daarin staan. Het belang van de eerbiediging van de persoonlijke levenssfeer, zoals bedoeld in artikel 5.1, tweede lid onder e, van de Woo, achten wij ten aanzien van deze gegevens groter dan het belang dat u heeft bij volledige openbaarmaking van de gevraagde documenten.
Wijze van openbaarmaking en publicatie

De documenten die (gedeeltelijk) openbaar worden, worden samen met deze brief de documenten digitaal aan u toegezonden.

Plaatsing op internet (HLTsamen tekst)
Het Woo-verzoekdit besluit en de drie documenten worden voor iedereen openbaar gemaakt door publicatie op de website van de gemeente www.hillegom.nl.

Vragen
Als u vragen heeft over de afhandeling van uw verzoek, dan kunt u contact opnemen met de woo-coördinator@hltsamen.nl . Voor meer informatie over de Woo-procedure, kunt u kijken op www.hillegom.nl.

Met vriendelijke groet,
namens burgemeester en wethouders van de gemeente Hillegom,

[redacted]
Woo-coördinator
Team Juridische Zaken

[redacted]

Van: [redacted]
Verzonden: dinsdag 9 november 2021 08:33
Aan: [redacted]
Onderwerp: Re: Kwetsbaarheden melden

Ha [redacted]

Die tekstuele toevoeging zal ik nog even doorgeven aan de redactie, dank! Wat betreft jouw vragen, ja dit is geborgd. Het mail adres wordt vanuit systeem- en netwerkbeheer elke werkdag gecheckt. Hier komen namelijk ook de kwetsbaarheidmeldingen vanuit leveranciers in terecht, dus mails in deze postbus hebben prio 1.

Met vriendelijke groet,
[redacted]
CISO - ENSIA Coördinator a.i.
Aanwezig: maandag, dinsdag en donderdag, vrijdag in overleg
Telefoon: [redacted]

Van: [redacted]
Verzonden: Monday, November 8, 2021 6:11:27 PM
Aan: [redacted]
Onderwerp: RE: Kwetsbaarheden melden
Hoi [redacted]
Hoewel ter info, heb ik toch twee vragen, een opmerking en een aanscherping m.b.t. de tekst. Zie de bijlage!
Kijk maar of je er wat mee kunt.
Groet, [redacted]

Van: [redacted]
Verzonden: donderdag 4 november 2021 12:32
Aan: [redacted]
Onderwerp: Kwetsbaarheden melden
Ha [redacted]
Ik kreeg van [redacted] de tip om dit even met je te delen, dus bij deze ☺
Ik heb zojuist overleg gehad met redactie en we gaan het bijgevoegde document op de website plaatsen.
Wat houd het in? De Coordinated Vulnarbility Disclosure (CVD) is een soort vrijwaring voor ethische hackers om kwetsbaarheden op onze systemen te melden.
Dit document is door het IBD gemaakt, ik heb enkel de HLT dingen er aan toegevoegd. Kwetsbaarheden kunnen straks via ZIVVER aan ons kenbaar gemaakt worden.
Het document komt op de drie gemeentelijke websites onder het privacybeleid. Dit is overigens ook een maatregel uit de BIO.
Dus in ieder geval bij deze ter info! Mocht je nog vragen hebben weet me te vinden.
Met vriendelijke groet,
[redacted]
CISO - ENSIA Coördinator a.i.
Aanwezig: maandag, dinsdag en donderdag, vrijdag in overleg
Telefoon: [redacted]

HLTsamen
Hillegom Lisse Teylingen

[redacted]

Van: [redacted]
Verzonden: woensdag 10 november 2021 07:46
Aan: HLTredactie
Onderwerp: RE: Kwetsbaarheden melden

Beste [redacted]

Dank voor het plaatsen!

Met vriendelijke groet,
Werkorganisatie HLTsamen

[redacted]
CISO & ENSIA coördinator a.i.

Aanwezig: maandag, dinsdag & donderdag, vrijdag in overleg
Telefoon: [redacted]

HLTsamen
Hillegom Lisse Teylingen

Van: HLTredactie
Verzonden: dinsdag 9 november 2021 17:25
Aan: [redacted]
Onderwerp: RE: Kwetsbaarheden melden

Beste [redacted]

Ik heb de teksten geplaatst op alle drie de websites. Bij 'Over deze website' en in de footer.

Met vriendelijke groet,
Werkorganisatie HLTsamen

[redacted]
Webredacteur
Team Communicatie, Bedrijfsvoering

Aanwezig op: Ma, Di, Do
Telefoon: [redacted]

HLTsamen
Hillegom Lisse Teylingen

Van: [redacted]
Verzonden: donderdag 4 november 2021 12:29

Aan: HLTredactie [redacted]
Onderwerp: RE: Kwetsbaarheden melden

Beste [redacted]

Hierbij het document. Ik heb de gemeente naam geel gearceerd, deze moet dan natuurlijk even aangepast worden per website.
Het betreft een maatregel vanuit de Baseline Informatie Veiligheid (BIO). In die zin is het inderdaad een verplichting voor de gemeenten om deze procedure te hebben en deze dus ook beschikbaar te stellen via onze website.

Met vriendelijke groet,

[redacted]
CISO - ENSIA Coördinator a.i.

Aanwezig: maandag, dinsdag en donderdag, vrijdag in overleg
Telefoon: [redacted]

HLTsamen
Hillegom Lisse Teylingen

Van: HLTredactie [redacted]
Verzonden: donderdag 28 oktober 2021 15:26
Aan: [redacted]
Onderwerp: RE: Kwetsbaarheden melden

Beste [redacted]

Wij kunnen deze informatie zeker plaatsen. Gaat het om een verplichting waar wij als gemeente aan moeten voldoen?
Als je ons de teksten stuurt zullen wij het plaatsen op de 3 websites.

Met vriendelijke groet,
Werkorganisatie HLTsamen

[redacted]
Webredacteur
Team Communicatie, Bedrijfsvoering

Aanwezig op: Ma, Di, Do
Telefoon: [redacted]

HLTsamen
Hillegom Lisse Teylingen

Van: [redacted]
Verzonden: maandag 18 oktober 2021 09:50
Aan: Communicatie [redacted]
Onderwerp: Kwetsbaarheden melden

Goedemorgen,

Graag begin ik eventjes kort met voorstellen. Ik ben [redacted] de vervanger van [redacted] Dit betekent dat ik mij bezig houd met de informatieveiligheid binnen HLTsamen.
In dat kader ben ik op zoek naar iemand die mij verder kan helpen met het volgende. Graag zou ik een voorstel doen om op de gemeente websites (Lisse, Hillegom en Teylingen) een kopje toe te voegen, bijvoorbeeld hier:

Postadres gemeente Lisse

Postbus 200

2160 AE Lisse

Meer contactgegevens →

Over deze website →

Toegankelijkheidsverklaring →

Privacyverklaring →

Gemeente Lisse op social media →

Huisregels Gemeentehuis Lisse →

We willen hiermee mensen uitnodigen en een 'escape' bieden om (technische) kwetsbaarheden te melden bij ons. Dit staat in de informatieveiligheidswereld beter bekend als de Responsible Disclosure.
Hierachter zou dan een tekst komen over de grenzen waarbinnen iemand moet blijven, logischerwijs mogen ze niet in onze informatie gaan zitten wroeten of onze systemen platleggen. Ik heb hier ook al een opzet voor klaarliggen.
Mijn vraag is dus concreet 1. Is dit mogelijk? En 2. Wie kan mij daar misschien bij helpen?
Alvast erg bedankt! ☺

Met vriendelijke groet,

[redacted]
CISO - ENSIA Coördinator a.i.

Aanwezig: dinsdag en donderdag, vrijdag in overleg
Telefoon: [redacted]

HLTsamen
Hillegom Lisse Teylingen

[redacted]

Van: [redacted]
Verzonden: woensdag 10 november 2021 09:06
Aan: [redacted]
CC: [redacted]
Onderwerp: RE: Kwetsbaarheden melden HLTsamen

Hallo [redacted]

Naar mijn inziens heeft dit geen keerzijde. In hackatons betreft het vaak een andere situatie. In een gecontroleerde omgeving wordt er dan geprobeerd om daadwerkelijk te penetreren en mogelijke data, inloggegevens, etc. buit te maken. De deelnemers hebben dan vanuit de hackaton een vrijwaring en geheimhoudingsplicht. In het geval van de CVD betreft het een andere aanpak.

De CVD is onderdeel van de BIO maatregelen en de IBD maakt hier al sinds 2017 gebruik van. Wij hebben dan ook hun standaard gebruikt om te zorgen dat we de juiste kaders meegeven voor wat wel en niet mag. Dat wat niet mag blijft, net zoals voorheen, strafbaar. Dit staat expliciet genoemd in de CVD. Dat wat wel mag heeft op geen enkele manier invloed op onze bedrijfsvoering, informatie en integriteit. We leggen hiermee een duidelijke grens neer voor de 'slechte' hackers. In mijn optiek is de CVD een soort 'meld misdaad' loket, maar dan voor cybercrime.

Met vriendelijke groet,
Werkorganisatie HLTsamen

[redacted]
CISO & ENSIA coördinator a.i.

Aanwezig: maandag, dinsdag & donderdag, vrijdag in overleg
Telefoon: [redacted]

HLTsamen
Hillegom Lisse Teylingen

Van: [redacted]
Verzonden: woensdag 10 november 2021 08:42
Aan: [redacted]
CC: [redacted]
Onderwerp: RE: Kwetsbaarheden melden HLTsamen

Hoi [redacted]

Ik herken dergelijke initiatieven die soms ook in een pressure cooker van 1 of paar dagen zitten van een hackaton.

Wat zou de keerzijde kunnen zijn van deze meer algemene en permanente oproep kunnen zijn ten aanzien van het aansporen van 'slechte' hackers?

Gr
[redacted]

Van: [redacted]
Verzonden: woensdag 10 november 2021 08:40
Aan: [redacted]

[redacted]
Onderwerp: Kwetsbaarheden melden HLTsamen

Beste [redacted] en [redacted]

Graag informeer ik jullie over een recentelijk ingericht proces voor informatieveiligheid. Ik heb hier afgelopen maandag reeds met de burgermeesters over gesproken. Bovendien halen we dit ook nog eens aan in de sessie van 25 november.
Onderstaande tekst heb ik zojuist op intranet gezet en beschrijft het onderwerp:

Sinds deze week staat er in de footer van de drie gemeentewebsites een uitnodiging en vrijwaring om kwetsbaarheden in onze systemen te melden.
In de informatiebeveiligingswereld staat dit fenomeen beter bekend als de **coordinated vulnerability disclosure (CVD)**. Hiermee nodigen we 'goede' hackers, ethische hackers, uit om kwetsbaarheden aan ons te melden. Hacken is normaliter strafbaar, maar als men binnen de perken van de CVD blijft zien wij af van de strafrechtelijke vervolging. Sterker nog, wij stellen ons juist dankbaar op tegenover deze personen. Zo werken we samen aan de weerbaarheid van HLTsamen en benutten we de kennis en kunde van onze samenleving.

Zie hier een voorbeeld van de CVD op de website van de gemeente Lisse:
Gemeente Lisse: Kwetsbaarheden melden

Behalve de interne communicatie ben ik nog met de redactie in gesprek om hier extern meer kenbaarheid aan te geven met bijvoorbeeld social media en/of het lokale krantje. Hier kan ik de 25e meer over vertellen.

Met vriendelijke groet,

[redacted]
CISO - ENSIA Coördinator a.i.

Aanwezig: maandag, dinsdag en donderdag, vrijdag in overleg
Telefoon: [redacted]