

J

**Van:** J  
**Verzonden:** donderdag 24 juni 2021 10:33  
**Aan:** J J  
**Onderwerp:** Beleid Coordinated Vulnerability disclosure 2021.docx  
**Bijlagen:** Beleid Coordinated Vulnerability disclosure 2021.docx

Hoi J en J

Vorig beveiligersoverleg hebben we ook het concept van het Vulnerability Disclosure beleid besproken en een openstaande vraag hierin is nog op welke wijze we deze (mogelijke) kwetsbaarheidsmeldingen willen gaan ontvangen.

Aangezien ook deze melding kunnen worden gezien als beveiligingsincident is het, het meest logisch om ook aan te sluiten bij de procedure 'incidentmeldingen'. De vraag is dan ook wat de gewenste wijze is waarop we graag willen dat deze content wordt aangeleverd en waar, zodat deze ook snel in topdesk kan worden opgenomen.

Ik zit zelf te denken aan de volgende opties:

- Via de website(s) dmv een webformulier in het Vulnerability beleid, welke direct wordt doorgezet naar topdesk ( voordeel dat we ook met een formulier goed benodigde (contact)gegevens kunnen uitvragen )
- Rechtstreeks naar een mailadres mailen vanuit de website ( wellicht vanuit IB niet meest gewenst )

Het incident kan via de reguliere incidentenprocedure worden beoordeeld, geprioriteerd en opgepakt, hierdoor verliezen we geen onnodige tijd en sluiten we aan bij een werkende procedure.

Het beleid is nogmaals bijgevoegd. De invulling van een eventuele beloning als dank voor de hulp is meer een keuze van het management van de gemeente zelf hoe men daar invulling aan wil geven, dat laat ik dan ook in besluitvorming graag aan hen over, maar de procedure van afwikkeling is mi wel aan ons.

Met vriendelijke groet,

J

J



J [@zevenaar.nl](mailto:J@zevenaar.nl)

0316-595 111  
Kerkstraat 27, 6901 AA Zevenaar  
Postbus 10, 6900 AA Zevenaar  
[www.zevenaar.nl](http://www.zevenaar.nl)

## Samenvatting Informatiebeveiligingsoverleg De Liemers – 29 juni 2021 (via Microsoft Teams)

Aanwezig:    en 

Afwezig: 

Voorzitter: 

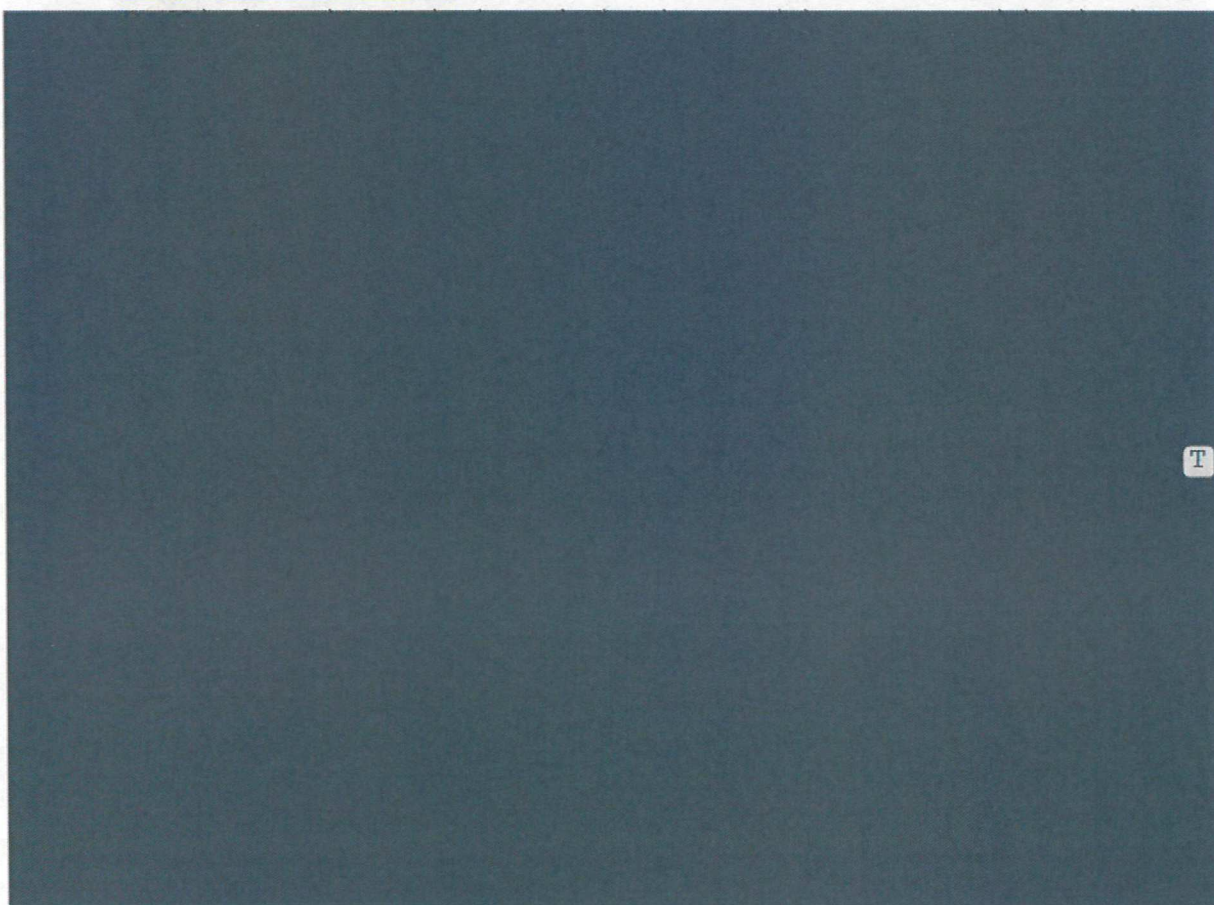
Secretaris: 

### 1. Opening, agenda en mededelingen

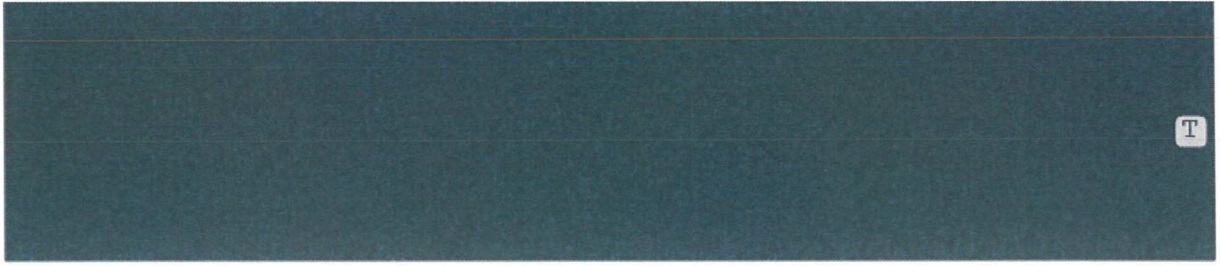
 is afwezig i.v.m. andere urgente werkzaamheden. De agenda wordt vastgesteld en er zijn geen aanvullende punten.



- b.  heeft het concept voor het Coordinated Vulnerability Disclosure beleid aangeleverd.  en  moeten hier nog een reactie op geven. Daarna kan het beleid per organisatie verder vastgesteld worden. > actie RID







**Van:** [redacted]  
**Verzonden:** donderdag 9 december 2021 10:18  
**Aan:** [redacted]  
**Onderwerp:** Vulnerability aanleveren contactgegevens

Hoi [redacted]

t.b.v het beleid Vulnerability Disclosure wat we op de nieuwe website willen publiceren ben ik even op zoek naar het juiste kanaal waar de signalen naartoe gezet kunnen worden.

We hebben dit afgelopen jaar al wel besproken binnen het beveiligingsoverleg en ook afgesproken dat deze meldingen zsm op de juiste plek moeten belangen maar ik heb nog geen antwoord op de volgende vragen:

Kun jij mij hier antwoord op geven ??

Het betreft hier het melden van kwetsbaarheden/zwakke plekken, onderstaande tekst komt oa op de website, op het heel gearceerde wil ik nog graag input:

1. Wat is het juiste mailadres waar de melding naartoe verzonden mag worden zodat deze direct op de juiste plek komt en gemeld/beoordeeld kan worden (topdesk), ( Wellicht dat dat straks ook gaat gebeuren dmv een contactforumlier maar ook dan moeten we wel weten waar deze naar toegezonden moet worden)
2. Is hier een versleutelmethodek waarnaar verwezen kan worden of hebben wij dit niet en moet dit verwijderd worden uit de tetsk ( zie ook bijgevoegde voorbeelden [VB1](#), [Vb2](#), )

----- gedeelte van de tekst zoals deze op de website gaat komen-----

*Gemeente Zevenaar hecht veel belang aan de beveiliging van haar systemen. Ondanks alle voorzorgsmaatregelen blijft het mogelijk dat een zwakke plek in de systemen te vinden is. Wanneer u een zwakke plek in één van onze systemen ontdekt, vernemen wij dit graag van u, zodat wij snel gepaste maatregelen kunnen nemen. Door het maken van een melding verklaart u zich als melder akkoord met onderstaande afspraken over Coordinated Vulnerability Disclosure en zal gemeente Zevenaar uw melding conform onderstaande afspraken afhandelen.*

*Wij vragen het volgende van u:*

- Mail uw bevindingen naar [Security@zevenaar](mailto:Security@zevenaar) Versleutel de bevindingen indien mogelijk met [<versleutelingsmethodek>](#) om te voorkomen dat de informatie in verkeerde handen valt.
- Geef voldoende informatie om het probleem te reproduceren, zodat we het zo snel mogelijk kunnen oplossen. Meestal is het IP-adres of de URL van het getroffen systeem en een omschrijving van de kwetsbaarheid voldoende, maar bij complexere kwetsbaarheden kan meer nodig zijn.
- Wij houden ons aanbevolen voor tips die ons helpen het probleem op te lossen. Beperkt u zich daarbij wel graag tot verifieerbare feitelijkheden die betrekking hebben op de door u geconstateerde kwetsbaarheid en vermijd dat uw advies in feite neerkomt op reclame voor specifieke (beveiligings)producten.
- Contactgegevens achter te laten zodat we met u in contact kunnen treden om samen te werken aan een veilig resultaat. Laat minimaal één e-mailadres of telefoonnummer achter.
- Dien de melding a.u.b. zo snel mogelijk in na ontdekking van de kwetsbaarheid.

----- einde tekstgedeelte -----

Met vriendelijke groet,



0316-595 111

Kerkstraat 27, 6901 AA Zevenaar

Postbus 10, 6900 AA Zevenaar

[www.zevenaar.nl](http://www.zevenaar.nl)

J

**Van:** J  
**Verzonden:** donderdag 28 april 2022 15:54  
**Aan:** Danielle Jansen  
**Onderwerp:** Beleidsdocumenten  
**Bijlagen:** T Beleid Coordinated  
Vulnerability disclosure 2022.pdf

Hoi Danielle,

Bijgevoegde beleidsdocumenten ter ondertekening.

Met vriendelijke groet,

J

J



J @zevenaar.nl  
0316-595 111  
Kerkstraat 27, 6901 AA Zevenaar  
Postbus 10, 6900 AA Zevenaar  
[www.zevenaar.nl](http://www.zevenaar.nl)

## Beleid Coördinated Vulnerability Disclosure

Het beleid Coördinated Vulnerability Disclosure (CVD) is onderdeel van het **strategisch informatiebeveiliging van de gemeente Zevenaar**. Het CVD dient in lijn te zijn met de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIO) en zal moeten voldoen aan de wettelijke regelgevingen en beleidsdocumenten van de gemeente Zevenaar.

Gemeente Zevenaar hecht veel belang aan de beveiliging van haar systemen. Ondanks alle voorzorgsmaatregelen blijft het mogelijk dat een zwakke plek in de systemen te vinden is. Wanneer u een zwakke plek in één van onze systemen ontdekt, vernemen wij dit graag van u, zodat wij snel gepaste maatregelen kunnen nemen. Door het maken van een melding verklaart u zich als melder akkoord met onderstaande afspraken over Coordinated Vulnerability Disclosure en zal gemeente Zevenaar uw melding conform onderstaande afspraken afhandelen.

### Wij vragen het volgende van u:

- Mail uw bevindingen naar [Security@zevenaar](mailto:Security@zevenaar). Versleutel de bevindingen indien mogelijk met een versleutelingsmethodiek om te voorkomen dat de informatie in verkeerde handen valt.
- Geef voldoende informatie om het probleem te reproduceren, zodat we het zo snel mogelijk kunnen oplossen. Meestal is het IP-adres of de URL van het getroffen systeem en een omschrijving van de kwetsbaarheid voldoende, maar bij complexere kwetsbaarheden kan meer nodig zijn.
- Wij houden ons aanbevolen voor tips die ons helpen het probleem op te lossen. Beperk u zich daarbij wel graag tot verifieerbare feitelijkheden die betrekking hebben op de door u geconstateerde kwetsbaarheid en vermijd dat uw advies in feite neerkomt op reclame voor specifieke (beveiligings)producten.
- Contactgegevens achter te laten zodat we met u in contact kunnen treden om samen te werken aan een veilig resultaat. Laat minimaal één e-mailadres of telefoonnummer achter.
- Dien de melding a.u.b. zo snel mogelijk in na ontdekking van de kwetsbaarheid.

### De volgende handelingen zijn niet toegestaan:

- Het plaatsen van malware, noch op onze systemen noch op die van anderen.
- Het zogeheten "bruteforcen" van toegang tot systemen
- Het gebruik maken van social engineering
- Het openbaar maken of aan derden verstrekken van informatie over het beveiligingsprobleem voordat het probleem is opgelost.
- Het verrichten van handelingen die verder gaan dan wat strikt noodzakelijk is om het beveiligingsprobleem aan te tonen en te melden. In het bijzonder waar het gaat om het verwerken (waaronder het inzien of kopiëren) van vertrouwelijke gegevens waar u door de kwetsbaarheid toegang toe heeft gehad. In plaats van een complete database te kopiëren, kunt u normaliter volstaan met bijvoorbeeld een directory listing. Het wijzigen of verwijderen van gegevens in het systeem is nooit toegestaan.
- Het gebruik maken van technieken waarmee de beschikbaarheid en/of bruikbaarheid van het systeem of services wordt verminderd (DoS-aanvallen).
- Het op wat voor (andere) wijze dan ook misbruik maken van de kwetsbaarheid.

#### Wat u mag verwachten:

- Indien u aan alle bovenstaande voorwaarden voldoet, zullen wij geen strafrechtelijke aangifte tegen u doen en ook geen civielrechtelijke zaak tegen u aanspannen.
- Als blijkt dat u een bovenstaande voorwaarde toch heeft geschonden, kunnen wij alsnog besluiten om gerechtelijke stappen tegen u te ondernemen.
- Wij behandelen een melding vertrouwelijk en delen persoonlijke gegevens van een melder niet zonder diens toestemming met derden, tenzij wij daar volgens de wet of een rechterlijke uitspraak toe verplicht zijn.
- Wij delen de ontvangen melding altijd met de Informatiebeveiligingsdienst voor gemeenten (IBD). Zo borgen wij dat gemeenten hun ervaringen op dit vlak met elkaar delen.
- In onderling overleg kunnen we, indien u dit wenst, uw naam vermelden als de ontdekker van de gemelde kwetsbaarheid. In alle andere gevallen blijft u anoniem.
- Wij sturen u binnen 1 werkdag een (automatische) ontvangstbevestiging.
- Wij reageren binnen 3 werkdagen op een melding met een (eerste) beoordeling van de melding en eventueel een verwachte datum voor een oplossing.
- Wij lossen het door u gemelde beveiligingsprobleem zo snel mogelijk op. Daarbij streven we ernaar om u goed op de hoogte te houden van de voortgang en nooit langer dan 90 dagen te doen over het oplossen van het probleem. Wij zijn daarbij vaak wel mede afhankelijk van toeleveranciers.
- In onderling overleg kan worden bepaald of en op welke wijze over het probleem wordt gepubliceerd, nadat het is opgelost.
- Wij kunnen u een beloning bieden als dank voor de hulp. Afhankelijk van de ernst van het beveiligingsprobleem en de kwaliteit van de melding, kan die beloning variëren van een eenvoudig 'dankjewel' tot een bedrag van maximaal €300,- euro. Het moet hierbij wel gaan om een nog onbekend en serieus beveiligingsprobleem.

Aldus vastgesteld door de algemeen Directeur/secretaris van de gemeente Zevenaar

| Datum      | Naam            | Handtekening                                                                         |
|------------|-----------------|--------------------------------------------------------------------------------------|
| 1 mei 2022 | Danielle Jansen |  |

# Toelichting grondslagen

In dit document kunt u secties terugvinden die onleesbaar zijn gemaakt. Deze informatie is achterwege gelaten op basis van de Wet open overheid (Woo). De letter die hierbij is vermeld correspondeert met de bijbehorende grondslag in onderstaand overzicht.

| Legenda verwijzing                                                                                                                                | Artikel verwijzing | Uitzonderingsgrond                                                                                                                                                                                                                                                                                                                            |
|---------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Artikel 5.1 lid 1 Woo – Absolute uitzonderingsgronden</b><br><b>De openbaarmaking van deze informatie:</b>                                     |                    |                                                                                                                                                                                                                                                                                                                                               |
| <b>A</b>                                                                                                                                          | art. 5.1 lid 1 a   | Kan de eenheid van de Kroon in gevaar brengen                                                                                                                                                                                                                                                                                                 |
| <b>B</b>                                                                                                                                          | art. 5.1 lid 1 b   | Kan de veiligheid van de Staat schaden                                                                                                                                                                                                                                                                                                        |
| <b>C</b>                                                                                                                                          | art. 5.1 lid 1 c   | Betreft bedrijfs- en fabricagegegevens die vertrouwelijk aan de overheid zijn meegedeeld                                                                                                                                                                                                                                                      |
| <b>D</b>                                                                                                                                          | art. 5.1 lid 1 d   | Betreft persoonsgegevens als bedoeld in paragraaf 3.1 (bijzondere persoonsgegevens) of paragraaf 3.2 (persoonsgegevens van strafrechtelijke aard) van de Uitvoeringswet Algemene verordening gegevensbescherming, waarvoor geen toestemming is gegeven of door de betrokkene kennelijk zelf openbaar zijn gemaakt                             |
| <b>E</b>                                                                                                                                          | art. 5.1 lid 1 e   | Het betreft nummers die dienen ter identificatie van personen die bij wet of algemene maatregel van bestuur zijn voorgeschreven als bedoeld in artikel 46 van de Uitvoeringswet Algemene verordening gegevensbescherming, tenzij de verstrekking kennelijk geen inbreuk op de levenssfeer maakt                                               |
| <b>Artikel 5.1 lid 2 Woo – Relatieve uitzonderingsgronden</b><br><b>Het belang van de openbaarmaking van deze informatie weegt niet op tegen:</b> |                    |                                                                                                                                                                                                                                                                                                                                               |
| <b>F</b>                                                                                                                                          | art. 5.1 lid 2 a   | Het belang van de betrekkingen van Nederland met andere staten en met internationale organisaties                                                                                                                                                                                                                                             |
| <b>G</b>                                                                                                                                          | art. 5.1 lid 2 b   | De economische of financiële belangen van de Staat, andere publiekrechtelijke lichamen of bestuursorganen                                                                                                                                                                                                                                     |
| <b>H</b>                                                                                                                                          | art. 5.1 lid 2 c   | Het belang van de opsporing en vervolging van strafbare feiten                                                                                                                                                                                                                                                                                |
| <b>I</b>                                                                                                                                          | art. 5.1 lid 2 d   | Het belang van de inspectie, controle en toezicht door bestuursorganen                                                                                                                                                                                                                                                                        |
| <b>J</b>                                                                                                                                          | art. 5.1 lid 2 e   | Het belang van de eerbiediging van de persoonlijke levenssfeer van betrokkenen                                                                                                                                                                                                                                                                |
| <b>K</b>                                                                                                                                          | art. 5.1 lid 2 f   | Het belang van de bescherming van andere dan in art. 5.1 lid 1 sub c genoemde concurrentiegevoelige bedrijfs- en fabricagegegevens                                                                                                                                                                                                            |
| <b>L</b>                                                                                                                                          | art. 5.1 lid 2 g   | Het belang van de bescherming van het milieu waar deze informatie betrekking op heeft                                                                                                                                                                                                                                                         |
| <b>M</b>                                                                                                                                          | art. 5.1 lid 2 h   | Het belang van de beveiliging van personen en bedrijven en het voorkomen van sabotage                                                                                                                                                                                                                                                         |
| <b>N</b>                                                                                                                                          | art. 5.1 lid 2 i   | Het belang van het goed functioneren van de Staat, andere publiekrechtelijke lichamen of bestuursorganen                                                                                                                                                                                                                                      |
| <b>O</b>                                                                                                                                          | art. 5.1 lid 4     | Het belang dat de geadresseerde erbij heeft om als eerste kennis te kunnen nemen van de informatie (tijdelijke beperking)                                                                                                                                                                                                                     |
| <b>P</b>                                                                                                                                          | art. 5.1 lid 5     | De onevenredige benadeling welke, in uitzonderlijke gevallen, wordt toegebracht aan een ander belang dan genoemd in art. 5.1 de leden 1 en 2, bij andere informatie dan milieu-informatie.                                                                                                                                                    |
| <b>Q</b>                                                                                                                                          | art. 5.1 lid 6     | Het belang genoemd in artikel 5.1 lid 1 c, het hier milieu-informatie betreft waardoor, bij openbaarmaking, ernstige schade wordt toegebracht aan het genoemde belang in artikel 5.1 lid 1c                                                                                                                                                   |
| <b>Artikel 5.2 lid 1 Woo – Persoonlijke beleidsopvattingen</b><br><b>De informatie uit documenten betreft:</b>                                    |                    |                                                                                                                                                                                                                                                                                                                                               |
| <b>R</b>                                                                                                                                          | art. 5.2 lid 1     | Persoonlijke beleidsopvattingen. Onder persoonlijke beleidsopvattingen worden verstaan ambtelijke adviezen, visies, standpunten en overwegingen ten behoeve van intern beraad, niet zijnde feiten, prognoses, beleidsalternatieven, de gevolgen van een bepaald beleidsalternatief of andere onderdelen met een overwegend objectief karakter |
| <b>S</b>                                                                                                                                          | Art. 5.2 lid 2     | Tot personen te herleiden gegevens, met betrekking tot door het bestuursorgaan, met het oog op een goede en democratische bestuursvoering, verstrekte informatie die kwalificeert als persoonlijke beleidsopvattingen                                                                                                                         |