



Samenwerkafspraken tussen toezichthouders en het NCSC

ten behoeve van de uitvoering
van de Cyberbeveiligingswet

7 oktober 2026



Partijen:

1. Autoriteit Nucleaire Veiligheid en Stralingsbescherming (ANVS)
2. Inspectie Gezondheidszorg en Jeugd (IGJ)
3. Inspectie Leefomgeving en Transport (ILT)
4. Inspectie van het Onderwijs¹ (IvHO)
5. Nederlandse Voedsel- en Warenautoriteit (NVWA)
6. Rijksinspectie Digitale Infrastructuur (RDI)

Partijen 1 t/m 6 hierna gezamenlijk ‘Toezichthouders’,

7. De Minister van Justitie en Veiligheid, te dezen vertegenwoordigd door het Nationaal Cyber Security Centrum, hierna ‘NCSC’

Overwegende dat:

- Toezichthouders van de ANVS, en de ambtenaren van IGJ, ILT, IvHO, NVWA en de RDI krachtens artikel 15 jo. 68, van de Cbw die zijn belast met het toezicht op de naleving van de Cbw door essentiële entiteiten, belangrijke entiteiten en leden van bestuur van essentiële en belangrijke entiteiten, én de ambtenaren van de RDI op grond van artikel 15 jo. 68 van de Cbw belast zijn met het toezicht op naleving van de Cbw door entiteiten die domeinnaamregistratiediensten verlenen. Hierna worden zij tezamen aangeduid als: toezichthouders;
- De toezichthouders en de minister van Justitie en Veiligheid, vertegenwoordigd door het NCSC, afspraken maken over de taken opgenomen in de Cbw en hiervoor met elkaar zullen afstemmen, samenwerken en informatie zullen uitwisselen;
- Het NCSC, op grond van artikel 16, tweede lid, Cbw, is aangewezen tot sectoraal CSIRT² voor een aantal sectoren, en tot taak heeft het verstrekken van vroegtijdige waarschuwingen, meldingen en aankondigingen en het verspreiden van informatie aan o.a. de toezichthouders;
- Het NCSC, op grond van artikel 14 Cbw, de rol als centraal contactpunt heeft (SPOC);
- Het NCSC, op grond van artikel 43 Cbw, namens de minister van Justitie en Veiligheid is aangewezen als beheerder van het nationaal register van entiteiten. Tevens is zij nationale uitvoeringscoördinator kwetsbaarheden en crisisbeheersing.
- De bevoegde autoriteiten en het NCSC op grond van artikel 51, eerste lid, Cbw een beginselplicht tot samenwerken hebben ten bate van een doeltreffende en doelmatige uitvoering van hun taken uit hoofde van de Cbw en daartoe onderling alle daarvoor noodzakelijke informatie, kennis en gegevens uitwisselen, waaronder persoonsgegevens;
- Op grond van het bepaalde in artikel 14 Cbw, de minister van Justitie en Veiligheid, het centrale contactpunt is, zoals bedoeld in artikel 8 van de NIS2 Richtlijn (Richtlijn (EU) 2022/2555). Deze taak wordt feitelijk uitgevoerd door het NCSC.

¹ Waarbij IvHO beoogd toezichthouder is.

² Informatiebeveiligingsdienst (IBD), Zorg- Computer Emergency Response Team (Z-CERT), Computer Emergency Response Team Water Management (CERT-WM) en SURF Computer Emergency Response Team (SURFcirt) zijn de andere sectorale CSIRTs.

Hoofdstuk 1 | Doel en definities

Artikel 1 | Definities

In dit document wordt verstaan onder:

- a. ANVS: de Autoriteit Nucleaire Veiligheid en Stralingsbescherming;
- b. AVG: Algemene Verordening Gegevensbescherming;
- c. Cbw: de Cyberbeveiligingswet, de Nederlandse wet ter implementatie van de NIS2;
- d. CSIRT: een Computer security incident response team, zoals bedoeld in artikel 16 van de Cbw;
- e. Datalek: een inbreuk in verband met persoonsgegevens (zoals bedoeld in artikel 4, onder punt 12 van de AVG), waarbij het waarschijnlijk is dat er een risico is ontstaan voor de rechten en vrijheden van natuurlijke personen (zoals bedoeld in artikel 33, lid 1 van de AVG);
- f. DTDW: overleg Directeuren Toezicht (Digitale) Weerbaarheid. Dit betreft het gremium waar de toezichthouders in samenwerken op directieurniveau sinds de oprichting in mei 2025;
- g. Entiteit: een entiteit zoals bedoeld in artikel 1, aanhef en 27e gedachtestreepje, Cbw;
- h. IGJ: de Inspectie Gezondheidszorg en Jeugd;
- i. ILT: de Inspectie Leefomgeving en Transport;
- j. IvHO: de Inspectie van het Onderwijs;
- k. NCSC: Nationaal Cyber Security Centrum;
- l. NIS2: richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van verordening (EU) (EU) nr. 910/2014 en richtlijn (EU) 2018/1972 en tot intrekking van richtlijn (EU) 2016/1148;
- m. NCTV: Nationaal Coördinator Terrorismebestrijding en Veiligheid;
- n. NVWA: de Nederlandse Voedsel- en Warenautoriteit;
- o. Register: lijst van essentiële en belangrijke entiteiten en entiteiten die domeinnaamregistratiediensten verlenen (richtlijn (EU) 2022/2555 overwegingen 18);
- p. RDI: de Rijksinspectie Digitale Infrastructuur;
- q. Samenloop van toezicht: indien een entiteit onder meerdere Cbw-sectoren valt en daardoor te maken krijgt met meer dan één toezichthouder;
- r. Significant incident: een incident zoals bedoeld in artikel 25 van de Cbw of een incident zoals bedoeld in artikel 17 van de Wwke;
- s. SPOC: Single Point of Contact;
- t. STDW: Samenwerking Toezichthouders (Digitale) Weerbaarheid. Dit betreft het gremium waar de Cbw toezichthouders (en Wwke-toezichthouders) in samenwerken onder het DTDW (f);
- u. Toezichthouder: de toezichthouders die bij ministeriële regeling, dan wel middels mandaatbesluit, zijn aangewezen en mandaat hebben om toezicht te houden op de naleving van de Cbw;
- v. Verplichte melding: Een melding die onder de meldplicht valt als bedoeld in artikel 25 van de Cbw, met inbegrip van de tussentijdse meldingen als bedoel in artikelen 26, 27, 28 en 2 Cbw;
- w. Vrijwillige melding: Een melding als bedoeld in artikel 33 van de Cbw;
- x. Wwke: Wet weerbaarheid kritieke entiteiten, de Nederlandse wet ter implementatie van de Europese Critical Entities Resilience Directive (Richtlijn (EU) 2022/2557 (CER).

Artikel 2 | Doel

De toezichthouders en het NCSC delen in het kader van deze wet hetzelfde maatschappelijke doel: de digitale veiligheid van Nederland te verhogen. Vanaf 15 augustus 2026 is de Cyberbeveiligingswet in werking getreden. Het NCSC en de toezichthouders hebben zowel plichten als bevoegdheden die volgen uit de Cbw (mede op basis van artikel 51 lid 1). Onderliggende samenwerkafspraken beogen de samenwerking ten behoeve van de taakuitoefening van partijen op grond van de Cbw en het maatschappelijke doel te ondersteunen en bevorderen.

Het doel van dit document is om tussen de toezichthouders en het NCSC samenwerkafspraken te maken en vast te leggen, om de doeltreffende en doelmatige uitvoering van de bevoegdheden die voortvloeien uit de Cbw te borgen en de digitale veiligheid van Nederland te verhogen.

Artikel 3 | Algemene uitgangspunten

1. De toezichthouders en het NCSC spannen zich zoveel als mogelijk in om elkaar te ondersteunen in situaties die de doeltreffende en doelmatige uitvoering van de Cbw versterken;
2. De inhoud van deze samenwerkafspraken is niet van toepassing op sectorspecifieke vereisten, tenzij de inhoud van dit document sectorspecifieke vereisten niet in de weg staat.

Artikel 4 | Verhouding met andere samenwerkafspraken

1. Indien en voor zover onderliggende samenwerkafspraken tegenstrijdig zijn met reeds bestaande afspraken, dan worden eventuele tegenstrijdigheden meegenomen in de eerstvolgende periodieke herziening dan wel in de evaluatie van de desbetreffende afspraken;
2. Een toezichthouder kan met een ander aangewezen CSIRT, anders dan het NCSC, specifieke afspraken voor een daar onder vallende sector maken. Dergelijke afspraken bestaan dan naast de in deze overeenkomst opgenomen afspraken.

Hoofdstuk 2 | Fundamentele uitgangspunten

Artikel 5 | Communicatie en delen informatie

De toezichthouders en het NCSC bevorderen adequate en tijdige onderlinge communicatie en gestructureerde informatiedeling, teneinde elkaar effectief te ondersteunen en te versterken bij de uitoefening van taken en bevoegdheden in het kader van de Cbw.

Artikel 6 | Contactpunt

De toezichthouders en het NCSC wijzen binnen hun organisatie een contactpunt aan dat geldt als het aanspreekpunt voor de samenwerkafspraken en al hetgeen daaruit voortvloeit.

Artikel 7 | Uitwisseling informatie

1. De toezichthouders en het NCSC organiseren ten minste tweemaal per jaar een overleg over de samenwerkingsafspraken in dit document;
2. Het voorgaande staat het organiseren van bilaterale overleggen of afstemmingen middels de gremia DTDW en het STWD niet in de weg;
3. Het DTDW en het STDW zijn samenwerkingsverbanden op initiatief van de toezichthouders. NCTV en NCSC nemen als toehoorder deel aan deze samenwerkingsverbanden;
4. Initiatieven voortkomend uit deze samenwerkingsverbanden worden, indien nodig, afgestemd op de in dit document vastgelegde samenwerkafspraken.

Hoofdstuk 3 | Registratie en gegevensuitwisseling

Artikel 8 | Registratie en gegevensuitwisseling

1. Toegang tot gegevens
 - a. De toezichthouders verkrijgen toegang tot het register van entiteiten, zoals beheerd door het NCSC, voor wat betreft de sector en/of het type entiteit waarvoor de toezichthouders zijn aangewezen;
 - b. In het geval dat de activiteiten van een entiteit onder meerdere toezichthouders of CSIRT's vallen, verkrijgen alle toezichthouders of CSIRT's toegang tot de registerinformatie van de betreffende entiteit;
 - c. Toezichthouders kunnen per (type) entiteit/sector, onderling bepalen of en wie de coördinerende toezichthouder wordt. De uitkomst hiervan wordt gedeeld met het NCSC ten behoeve van de juistheid van registratie.
2. Uitwisseling van gegevens
 - a. Overeenkomstig artikel 51 Cbw, wisselen partijen onderling informatie uit, waaronder persoonsgegevens;
 - b. Gegevensuitwisseling vindt plaats via geijkte kanalen;
 - c. In het geval van het uitwisselen van persoonsgegevens bewaken partijen de kaders zoals vastgelegd bij of krachtens de AVG en daarmee verband houdende jurisprudentie en wordt aangesloten bij de daarin opgenomen definities;
 - d. Partijen zijn zelfstandig verwerkingsverantwoordelijken (in de zin van artikel 4 onder 7 AVG) en waarborgen zelfstandig de rechten van betrokkenen;
 - e. De verstrekking van persoonsgegevens wordt, voor zover dit passend en geboden is, door de verzender zodanig doelmatig of noodzakelijk gepseudonimiseerd middels hashes of anderszins toegepaste encryptie dat de betrokkene door de ontvanger niet geïdentificeerd kan worden;
 - f. De verzender van IP-adressen stelt indien deze (indirect) als persoonsgegeven kwalificeren voorafgaand aan de verzending de ontvanger daarvan in kennis. Voor zover dit passend en geboden is, treft de verzender aanvullende maatregelen om te voorkomen dat de betrokkene geïdentificeerd kan worden;
 - g. Overeenkomstig het bepaalde in artikel 43, lid 3, Cbw kan het NCSC, als beheerder van het register, in overeenstemming met de betrokken toezichthouder(s) een registratie wijzigen, weigeren of beëindigen;
 - h. *[gereserveerd voor uitkomst validatieproces VAV. Deze punten worden bij de eerste evaluatie (artikel 14) aangevuld.]*

Hoofdstuk 4 | Meldingen

Artikel 9 | Toegang tot gegevens

1. Toegang tot gegevens
 - a. Toezichthouders krijgen direct toegang tot de informatie over verplichte meldingen via het meldportaal van het NCSC, voor zover deze meldingen betrekking hebben op de sector en/of type entiteit waarvoor de toezichthouder is aangewezen;
 - b. Vrijwillige meldingen worden gedeeld met de desbetreffende toezichthouder(s), mits de meldende partij hiervoor nadrukkelijke toestemming geeft bij de melding in het meldportaal;
 - c. In geval van verplicht gedane meldingen door entiteiten die onder meerdere toezichthouders of CSIRT's vallen, verkrijgen die toezichthouders en CSIRT's, overeenkomstig het bepaalde in artikel 8.1, onder b, toegang tot deze melding.
2. Uitwisseling van (persoons)gegevens Cbw
 1. Het melden van vermoedelijke datalekken bij entiteiten uit het register, waarvan ofwel het CSIRT, ofwel de betrokken toezichthouder bij de uitoefening van de wettelijke taken kennis krijgt, is en blijft een verantwoordelijkheid van de betreffende entiteit;
 2. Indien bij de uitwisseling van informatie sprake is van persoonsgegevens, dan is de AVG daarop van toepassing.

Hoofdstuk 5 | Incidentmanagement en crisisbeheersing

Artikel 10 | Incidentmanagement en crisisbeheersing

1. Het NCSC stuurt bij een verplichte melding automatisch de informatie die de entiteit of entiteiten hebben gedeeld, door aan de relevante toezichthouder(s);
2. Mocht tijdens een incident - waarbij het NCSC het bevoegde CSIRT is - een toezichthouder actief toezicht willen opzetten, wordt het NCSC onverwijld hiervan op de hoogte gesteld, teneinde de afstemming over het incident te versoepelen;
3. Tijdens een incident kan een toezichthouder bij het NCSC vragen of het NCSC actief betrokken is. Hierop kan door het NCSC louter ontkennend of bevestigend worden gereageerd. Aanvullende informatie verkrijgt de betrokken toezichthouder(s) middels het NCSC-portaal als bedoeld onder lid 1 van dit artikel;
4. Te allen tijde kan een toezichthouder een hulpverzoek indienen bij het NCSC voor een vorm van ondersteuning (zoals bijvoorbeeld technische informatieduiding);
5. Het NCSC brengt de betrokken toezichthouder(s) zo spoedig mogelijk op de hoogte wanneer een incident met grensoverschrijdende gevolgen internationaal wordt gedeeld met het relevante SPOC van het specifieke land, zoals bedoeld in artikel 39 van de Cbw.

Hoofdstuk 6 | (Grensoverschrijdende) informatiedeling

Artikel 11 | (Grensoverschrijdende) informatiedeling

1. Op verzoek van een sectorale CSIRT of betrokken toezichthouder stuurt het NCSC als centrale contactpunt meldingen door naar centrale contactpunten van andere potentiële betrokken lidstaten, zoals bedoeld in artikel 39, derde lid, Cbw;
2. De betrokken toezichthouder kan, na raadpleging van de betrokken entiteit, het publiek informeren over een significant incident of de entiteit verplichten om dit te doen, wanneer:
 - a. publieke bewustmaking nodig is om meerdere significante incidenten te voorkomen;
 - b. dat nodig is om een lopend incident te beheersen; of
 - c. de bekendmaking van het significante incident anderszins in het algemeen belang is (39, derde lid, Cbw);

De toezichthouder stelt waar mogelijk hiervan het relevante CSIRT vooraf op de hoogte van deze voorgenomen publieke bekendmaking;
3. De toezichthouders en het NCSC verstrekken informatie aan elkaar, die enkel wordt gebruikt overeenkomstig het doel van de verstrekking, behoudens voor zover wettelijk voorschrijft hen tot mededeling aan een derde partij verplicht.

Hoofdstuk 7 | Kennisuitwisseling

Artikel 12 | Kennis

1. De toezichthouders en het NCSC wisselen kennis uit;
2. Kennisuitwisseling heeft tot doel om de kwaliteit en consistentie van kennisproducten, adviezen en sectorbeelden te versterken, de toezichthouders te ondersteunen bij de uitoefening van hun toezichttaak en te zorgen voor eenduidige communicatie richting de entiteiten en naar de maatschappij. De gezamenlijke kennisopbouw draagt daarmee bij aan beter onderbouwde risicoanalyses, scherpere prioritering, effectieve interventies en een consistente duiding van ontwikkelingen binnen en over de sectoren heen;
3. De volgende activiteiten in het kader van kennisuitwisseling zijn onderkend (niet limitatief):
 - a. Structurele en tijdige uitwisseling van relevante informatie over dreigingen, incidenten, kwetsbaarheden en trends, binnen de geldende wettelijke kaders mogelijk te maken;
 - b. Het uitwisselen van informatie over het volwassenheidsniveau van sectoren/sectorbeelden op het gebied van digitale weerbaarheid;
 - c. Afstemming dan wel gezamenlijke ontwikkeling en actualisatie van sectorbeelden en overkoepelende dreigings- en risicoanalyses;
 - d. Informeren over prioriteiten en focusgebieden in jaarplannen, toezichtagenda's en uitvoeringsprogramma's;
 - e. Gecoördineerde communicatie richting de maatschappij ten behoeve van preventieve onderwerpen, waar passend;
 - f. Periodieke evaluatie (gekoppeld aan de evaluatiecyclus van deze set van samenwerkafspraken) van de samenwerking en kennisuitwisseling, gericht op continue verbetering;
 - g. Vrijwillige meldingen worden, indien en voor zover door de melder niet overeenkomstig artikel 9 lid 1 sub b is aangegeven dat deze met de toezichthouder mag worden gedeeld, geanonimiseerd en geaggregeerd – en indien mogelijk gekoppeld aan de sector of subsector – maandelijks gedeeld met voor die sector of sectoren aangewezen toezichthouders;
 - h. Bij alle vormen van informatie-uitwisseling wordt zorgvuldig in acht genomen dat geen informatie wordt gedeeld die herleidbaar is tot individuele entiteiten of specifieke doelgroepen, tenzij hiervoor een toereikende wettelijke grondslag bestaat.

Hoofdstuk 8 | Slotbepalingen

Artikel 13 | Resolutiemechanisme

1. Als er tussen toezichthouders en het NCSC over deze samenwerkafspraken een verschil van inzicht ontstaat over de uitleg, uitvoering of toepassing, of over de daarmee samenhangende afspraken, treden de partijen zo spoedig mogelijk met elkaar in overleg om tot een oplossing te komen;
2. Indien het overleg zoals bedoeld in lid 1 van dit artikel niet leidt tot een voor alle partijen aanvaardbare oplossing, wordt het verschil van inzicht voorgelegd aan het bestuurlijke niveau van de betrokken partijen;
3. Zolang het verschil van inzicht niet is opgelost, blijven de betrokken partijen zich inspannen om de uitvoering van dit document, voor zover redelijkerwijs mogelijk, onverminderd voort te zetten;
4. Dit resolutiemechanisme laat onverlet de wettelijke verantwoordelijkheden van elke partij bij dit document.

Artikel 14 | Evaluatie

Partijen zullen een jaar na de inwerkingtreding van de Cbw, en vervolgens in ieder geval elke drie jaar, de uitvoering en effectiviteit van deze samenwerkafspraken evalueren.

Artikel 15 | Verdere uitwerking

De verdere uitwerking en toepassing van hetgeen is afgesproken in deze samenwerkafspraken, waaronder de werkafspraken zoals genoemd in artikel 5, vinden plaats in het overleg STDW.

Artikel 16 | Inwerkingtreding en looptijd

1. Deze samenwerkovereenkomst treedt gelijktijdig met de Cbw in werking en wordt voor onbepaalde tijd aangegaan;
2. Deze set van samenwerkafspraken kan in onderlinge overeenstemming tussen alle partijen worden gewijzigd.

Uitgave

Nationaal Cyber Security Centrum (NCSC)
Postbus 117, 2501 CC Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5555

Meer informatie

www.ncsc.nl
info@ncsc.nl
[@ncsc_nl](https://twitter.com/ncsc_nl)

oktober 2026