



IVP-bouwstenen Digitale veiligheid

Datum: 15-10-2026

Doel van dit document

Deze notitie ondersteunt gemeenten bij het opstellen van hun ambitie op het gebied van digitale veiligheid in het IVP. De opgenomen ambities en doelstellingen sluiten aan bij de regionale koers voor 2027-2030. Gemeenten kunnen de bouwstenen rechtstreeks gebruiken in hun IVP en deze aanvullen met elementen uit deze achtergrondnotitie die aansluiten bij de lokale situatie.

Wat zien we?

Digitale veiligheid raakt iedere inwoner

- Digitalisering biedt inwoners, ondernemers en maatschappelijke organisaties veel kansen, maar maakt hen ook kwetsbaar voor nieuwe vormen van criminaliteit. Online criminaliteit groeit al jaren: 40% van alle criminaliteitsslachtoffers is slachtoffer van een online delict.
- Ook in onze gemeente hebben inwoners en ondernemers te maken met digitale dreigingen. Online criminaliteit beperkt zich niet tot de digitale wereld, maar heeft directe gevolgen voor het dagelijks leven. Slachtoffers kunnen financiële schade oplopen, emotionele problemen ervaren en het vertrouwen in organisaties verliezen.
- Tegelijkertijd blijft een groot deel van de online criminaliteit buiten beeld doordat slachtoffers geen melding of aangifte doen. Hierdoor is het werkelijke probleem groter dan officiële cijfers laten zien.

Online criminaliteit ontwikkelt zich snel

- Criminelen maken steeds professioneler gebruik van digitale middelen. Online fraude, phishing, bankhelpdeskfraude, ransomware en sextortion worden op grote schaal uitgevoerd.
- Daarnaast worden digitale middelen steeds vaker ingezet bij traditionele vormen van criminaliteit, zoals fraude, ondermijning, intimidatie en geweld.
- Nieuwe technologieën, zoals kunstmatige intelligentie (AI), vergroten de snelheid, toegankelijkheid en geloofwaardigheid van deze criminaliteit.

Een integrale aanpak is noodzakelijk

- Digitale veiligheid raakt meerdere beleidsterreinen. De online en fysieke leefwereld zijn nauw met elkaar verweven, waardoor vraagstukken rondom veiligheid, jeugd, onderwijs, economie en zorg steeds vaker een digitale component bevatten.
- Digitale veiligheid is daarmee niet langer een afzonderlijk thema, maar een integraal onderdeel van het veiligheidsbeleid.
- Online criminaliteit houdt zich bovendien niet aan gemeentegrenzen. Slachtoffers, daders en relevante signalen bevinden zich vaak in verschillende gemeenten, regio's of landen. Hierdoor zijn samenwerking, kennisdeling en een gezamenlijke aanpak met andere gemeenten en partners noodzakelijk.

Waar willen we naartoe en hoe bereiken we dit?

De onderstaande doelen en bouwstenen kunnen worden opgenomen in het Integraal Veiligheidsplan en aangepast aan de lokale situatie, prioriteiten en bestaande samenwerkingsstructuren.

1. Inwoners en ondernemers zijn digitaal weerbaar

Waar willen we naartoe?

- Inwoners en ondernemers zijn digitaal weerbaar en bewust van digitale risico's.
- Kwetsbare groepen beschikken over voldoende kennis en vaardigheden om zich tegen online criminaliteit te beschermen.
- Jongeren raken niet betrokken bij digitale criminaliteit en zijn weerbaar tegen verleidingen en ronselpraktijken.

Hoe bereiken we dit?

- We stimuleren inwoners en ondernemers om hun digitale weerbaarheid en bewustwording te vergroten.
- We zetten in op voorlichting en preventie, waarbij we inwoners actief informeren over digitale risico's en handelingsperspectief bieden.
- We creëren bewustwording bij jongeren over de risico's en gevolgen van online criminaliteit en versterken hun weerbaarheid tegen verleidingen en ronselpraktijken.
- We werken samen met maatschappelijke organisaties, onderwijsinstellingen en ondernemersnetwerken om verschillende doelgroepen effectief te bereiken.

2. Slachtoffers ontvangen tijdig passende ondersteuning

Waar willen we naartoe?

- Slachtoffers weten de weg naar hulp en ondersteuning goed te vinden, zodat ze snel passende nazorg ontvangen.
- De impact van slachtofferschap wordt beperkt en de kans op herhaald slachtofferschap verkleint.

Hoe bereiken we dit?

- We zorgen met onder meer politie, Slachtofferhulp Nederland en andere relevante partners voor heldere hulproutes, goede doorverwijzing en passende ondersteuning, zodat slachtoffers sneller de juiste hulp ontvangen.
- We versterken de herkenning van online criminaliteit onder professionals die in contact staan met inwoners, zodat zij slachtoffers kunnen begeleiden naar passende hulp en hen waar nodig kunnen stimuleren om melding of aangifte te doen.

3. Partners beschikken over een gezamenlijk beeld van risico's en ontwikkelingen

Waar willen we naartoe?

- Partners beschikken over een gezamenlijk en actueel beeld van risico's, doelgroepen en ontwikkelingen. Signalen en informatie uit verschillende organisaties worden beter aan elkaar verbonden.
- Er is een samenhangende aanpak die slachtofferschap voorkomt, daderschap ontmoedigt en digitale weerbaarheid vergroot.

Hoe willen we dit bereiken?

- We werken samen met politie, onderwijsinstellingen, maatschappelijke organisaties, ondernemers en andere relevante partners.
- We delen, waar wet- en regelgeving dit toestaat, kennis, signalen en ervaringen en versterken daarmee onze gezamenlijke informatiepositie.
- We combineren beschikbare data met signalen uit de lokale praktijk om ontwikkelingen en risico's vroegtijdig te herkennen.
- Op basis van dit gezamenlijke beeld zetten we gerichte preventieve interventies en andere passende maatregelen in.
- We sluiten aan bij regionale en landelijke samenwerkingsverbanden om kennis te delen, ontwikkelingen te duiden en gezamenlijk op te treden waar dat meerwaarde biedt.

Meer achtergrondinformatie nodig?

Wilt u uw IVP verder onderbouwen of lokale accenten toevoegen? Raadpleeg dan de bijlage [*Achtergrondinformatie Digitale Veiligheid voor het IVP*](#). Deze bevat aanvullende informatie over ontwikkelingen, risico's, slachtofferschap, daderschap en samenwerkingsvraagstukken rondom online criminaliteit.

Ook deze webpagina's zijn aan te bevelen om te raadplegen:

- [Agenda digitale veiligheid - VNG](#)
- [Integraal veiligheidsplan maken - Het CCV](#)