Datum
16 april 2026

Bestuurlijk Beleidskader
Fysieke Beveiliging 2026-2030

Inhoud

Voorwoord

Het waterschap AGV vervult een essentiële rol in het waarborgen van waterveiligheid, waterkwaliteit en waterkwantiteit. De continuïteit van deze dienstverlening vraagt om robuuste en aantoonbare weerbaarheid tegen fysieke dreigingen.

Met de inwerkingtreding van de Wet weerbaarheid kritieke entiteiten (Wwke) wordt het waterschap aangewezen als kritieke entiteit. Deze wet is de Nederlandse implementatie van de Europese CER-richtlijn (Critical Entities Resilience) en heeft als doel de fysieke weerbaarheid van organisaties die essentiële diensten leveren structureel te versterken.

De Wwke vraagt van kritieke entiteiten dat zij periodiek een risicobeoordeling uitvoeren (all hazards), passende en evenredige maatregelen treffen (zorgplicht), incidenten die de essentiële dienstverlening verstoren of kunnen verstoren tijdig melden en hierover verslagleggen, en dat zij aantoonbaar in control zijn richting toezicht.

Dit Bestuurlijk Beleidskader Fysieke Beveiliging 2026 – 2030 geeft richting aan hoe wij deze verplichtingen borgen en onze weerbaarheid in de praktijk versterken.

1 Aanleiding

Het waterschap AGV is verantwoordelijk voor taken die direct raken aan de veiligheid en het welzijn van inwoners, bedrijven en de leefomgeving. Het beheren van waterkeringen, het regelen van peilen, het zuiveren van afvalwater en het borgen van voldoende water vraagt om betrouwbare processen, bestuurbare assets en een organisatie die ook onder verstorende omstandigheden kan blijven functioneren.

Fysieke dreigingen—zoals inbraak, sabotage, vandalisme, diefstal, intimidatie, brandstichting en doelgerichte verstoring—kunnen de continuïteit van deze essentiële dienstverlening direct aantasten. Daarnaast kunnen fysieke incidenten leiden tot effecten op procesautomatisering en informatiesystemen, waardoor fysieke en digitale weerbaarheid in de praktijk onlosmakelijk met elkaar verbonden zijn.

De Wet weerbaarheid kritieke entiteiten (Wwke) geeft een duidelijke wettelijke basis aan deze opgave. De Wwke is de Nederlandse vertaling van de Europese CER-richtlijn (Critical Entities Resilience) en richt zich op het vergroten van de fysieke weerbaarheid van organisaties die essentieel zijn voor de samenleving.

Een bijzonder actueel aandachtspunt is de ontvlechting van Waternet. Essentiële functies zoals beveiligingsdienstverlening, toegangsmiddelenbeheer, functioneel beheer, contractmanagement van beveiligingsdiensten en technisch applicatiebeheer van beveiligingssystemen moeten gecontroleerd worden overgenomen, zonder verlies van continuïteit, kennis, registraties of sturing.

Voor het waterschap betekent dit dat fysieke beveiliging niet meer alleen een interne beheersingsmaatregel is, maar een wettelijke verplichting die aantoonbaar moet worden ingevuld.

Dit bestuurlijk beleidskader Fysieke Beveiliging 2026–2030 beschrijft de koers en de belangrijkste thema’s voor de komende vijf jaar. Het geeft daarnaast richting aan de inrichting van de organisatie en de verantwoordelijkheidsverdeling.

2 Wettelijk kader

2.1 Wet weerbaarheid kritiek entiteiten

Bij waterschappen zijn de processen Keren en Beheren en Afvalwater als vitaal geclassificeerd. Daarmee zijn deze processen (en datgene wat we daarvoor doen) aangemerkt als essentieel voor het voorkomen van maatschappelijke ontwrichting en het borgen van veiligheid, volksgezondheid en continuïteit van dienstverlening. Deze classificatie betekent dat het waterschap zich voorbereidt op en moet kunnen aantonen dat het voldoet aan de (aanvullende) verplichtingen die voortvloeien uit de Wet weerbaarheid kritieke entiteiten.

De fysieke beveiliging sluit aan op en ondersteunt:

- Wet weerbaarheid kritieke entiteiten (Wwke): verplichtingen voor risicobeoordeling fysieke risico's, zorgplicht (passende en evenredige organisatorische, elektronische en bouwkundige beveiligingsmaatregelen), incidentmelding en verslaglegging, en toezicht/auditaarbaarheid.
- Besluit weerbaarheid kritieke entiteiten met regels voor de uitvoering van de Wet weerbaarheid kritieke entiteiten.
- Cyberbeveiligingswet: verplichtingen voor bestuurlijke verantwoordelijkheid, registratieplicht, zorgplicht (passende en evenredige technische, operationele en organisatorische maatregelen voor de beveiliging van de netwerk- en informatiesystemen), meldplicht, en toezicht/auditeerbaarheid.
- Arbeidsomstandighedenwet (Arbowetgeving): veilige werkomgeving, beheersing van agressie/geweld en veilige processen voor medewerkers en contractors.
- Privacywetgeving (AVG): eisen rond cameratoezicht, logging, doelbinding, toegangsrechten tot beelden/logs, bewaartermijnen en DPIA's waar nodig.
- Archiefwet: bewaarplichten voor relevante registraties, besluitvorming en incidentdossiers.
- WPG: Wet politiegegevens.
- Aanpalende veiligheids- en crisiswetgeving: interne crisisorganisatie en samenwerking met ketenpartners en publieke veiligheidspartners.

2.2 Eigen risicobeoordeling (all hazards)

- Er is een organisatiebrede risicobeoordeling voor alle relevante dreigingen die essentiële dienstverlening kunnen verstoren.
- De risicobeoordeling is tijdig uitgevoerd binnen de wettelijke termijn na aanwijzing en wordt ieder 4 jaar herhaald en/of geactualiseerd bij relevante wijzigingen.

2.3 Zorgplicht: passende en evenredige maatregelen

- Op basis van de risicobeoordeling is een maatregelenpakket vastgesteld dat preventie, detectie, respons en herstel omvat.
- Er is een meerjarig maatregelenplan met prioriteiten, eigenaren, termijnen en beoogde risicoreductie.
- Afwijkingen en restrisico's worden expliciet vastgelegd en door het bevoegde niveau geaccepteerd.

2.4 Incidentmelding en verslaglegging

- Incidenten die de essentiële dienstverlening verstoren of kunnen verstoren worden zonder onnodige vertraging gemeld via een vastgesteld meldproces.

- Voor elk meldplichtig incident wordt binnen de wettelijke termijn een gedetailleerd verslag opgeleverd (impact, aard, oorzaken, gevolgen, genomen maatregelen en vervolgacties).
- Het proces is geoefend en werkt aantoonbaar (rollen, contactpunten, registratie, kwaliteitscontrole).

2.5 Toezicht, handhaving en auditbaarheid

- De organisatie is audit-ready: bewijsvoering, registraties en besluitvorming zijn volledig en actueel.
- Onafhankelijke toetsing kan snel worden ingericht en opgevolgd met verbetermaatregelen.

3 Bestuurlijk beleidskader

Het bestuurlijke beleidskader bestaat uit de volgende vijf leidende principes:

3.1 Veiligheid van personen en continuïteit van dienstverlening staat voorop
Alle fysieke beveiligingsmaatregelen zijn primair gericht op het beschermen van medewerkers, bezoekers en contractors én op het waarborgen van de continuïteit van de dienstverlening. Bij spanningen tussen belangen in de organisatie krijgt de fysieke veiligheid van personen altijd prioriteit. Het beleid borgt daarnaast dat situaties met direct gevaar of (dreigende) verstoring van de dienstverlening tijdig worden herkend, dat passende preventieve en mitigerende maatregelen worden genomen en dat er heldere escalatie-, crisis- en ontruimingsafspraken zijn om de impact op mensen, middelen en processen te beperken.

3.2 Risicogestuurd, proportioneel en herleidbaar (maatregelkeuze en restrisico)
Fysieke beveiligingsmaatregelen worden gekozen op basis van aantoonbare risico's: dreiging, kwetsbaarheid en impact. De zwaarte van maatregelen is proportioneel: niet zwaarder dan nodig, maar voldoende om het risico tot een acceptabel niveau te brengen. De onderbouwing is herleidbaar: per maatregel is duidelijk waarom deze is gekozen, welke alternatieven zijn overwogen en welk restrisico resteert (inclusief acceptatie door de juiste eigenaar).

3.3 Preventie is de basis, detectie en respons sluiten hierop aan
De inrichting van fysieke beveiliging volgt een logische keten: eerst voorkomen, vervolgens tijdig signaleren en tot slot adequaat handelen. Preventieve maatregelen beperken de kans op incidenten (bijv. barrières, procedures, bewustwording). Detectiemiddelen maken afwijkingen zichtbaar (bijv. alarmering, toezicht, monitoring). Respons zorgt voor snelle en passende opvolging (bijv. interventie, opschaling, incidentafhandeling).

3.4 Laag-op-laag beveiliging (perimeter–gebouw–kritieke ruimte–kritieke asset)
Beveiliging wordt opgebouwd in meerdere, elkaar versterkende lagen. Hoe dichter bij de kritieke processen en assets, hoe specifieker en strenger de maatregelen. Dit voorkomt "single points of failure" en maakt het moeilijker om ongeautoriseerd door te dringen. Elke laag heeft een eigen doel: weren aan de buitenzijde, beheersen in het gebouw, afschermen van kritieke ruimten en beschermen van kritieke assets.

3.5 Strikt toegangsbeheer (uitgifte, intrekking, review, logging)
Toegang tot locaties, ruimten en assets wordt strikt beheerd volgens "need-to-have/need-to-be-there". Dit omvat gecontroleerde uitgifte van middelen (passen/sleutels/credentials), snelle intrekking bij functiewijziging of uitdiensttreding, periodieke reviews op rechten en autorisaties, en volledige logging zodat toegang en afwijkingen achteraf te reconstrueren en te onderzoeken zijn.

4 Doel en ambitie

Het doel is om de continuïteit van essentiële dienstverlening te borgen en de veiligheid van personen, vitale assets en kritieke processen te beschermen tegen fysieke dreigingen.

4.1 Ambitie 2026–2030

- Fysieke beveiliging is aantoonbaar effectief, risico gestuurd en uniform georganiseerd.
- Vitale processen en installaties zijn aantoonbaar beschermd met passende en evenredige maatregelen.
- Incidenten worden tijdig gedetecteerd, opgevolgd en gerapporteerd; verbetering is structureel geborgd.
- Het waterschap voldoet aantoonbaar aan de verplichtingen uit de Wet weerbaarheid kritieke entiteiten en relevante aanpalende wet- en regelgeving.

4.2 Reikwijdte en afbakening

Het kader richt zich op de fysieke en menselijke toegangspoort. De logische toegangspoort (IT/OT/cyber) valt onder informatiebeveiliging, maar wordt integraal afgestemd, omdat fysieke toegang direct van invloed is op cyber- en IT/-OT-risico's.

Dit kader geldt voor:

- Alle locaties en assets die nodig zijn voor essentiële diensten, waaronder waterkeringen, gemalen, stuwen/sluizen, RWZI's, bedienlocaties, kantoren, magazijnen, werkplaatsen en steunpunten.
- Alle personen die toegang hebben tot locaties en middelen: medewerkers, contractpartijen, leveranciers, bezoekers en partners.
- Alle fysieke beveiligingsmaatregelen: bouwkundig, elektronisch en organisatorisch, inclusief toezicht, toegangsbeheer, procedures, opvolging en beheer/onderhoud.

4.3 Normeringen (richtinggevend)

De normeringslijn bestaat uit:

- ISO 31000 voor risicomanagement
- ISO 22301 voor business continuity management
- ISO 22336 voor Security & Resilience
- ISO 22316 voor het versterken van de weerbaarheid
- Cybersecurity Implementatierichtlijn voor fysieke beveiligingseisen (CSIR)
- Baseline Informatiebeveiliging Overheid voor beveiliging van informatie en netwerk en informatiesystemen (BIO2)
- ISO 27001 en ISO 27002 beveiligingsstandaarden
- IEC62443 voor informatiebeveiliging en fysieke beveiliging van procesautomatisering.

4.4 Integraal samenwerken

Fysieke beveiliging is onderdeel van een bredere weerbaarheid en wordt integraal ingericht met betrokken disciplines. Afstemming met risicomanagement, informatiebeveiliging, crisismanagement, facilitaire zaken en assetmanagement zorgt voor consistente keuzes (bijv. classificatie, kritikaliteit, onboarding/offboarding, incidentrespons). Rollen, verantwoordelijkheden en overdrachtsmomenten zijn expliciet vastgelegd, zodat preventie, detectie en respons naadloos op elkaar aansluiten.

4.5 Risicomanagement

Het doel van risicomanagement voor fysieke beveiliging is gericht op personen, bedrijfscontinuïteit, processen, dienstverlening en bedrijfsmiddelen tijdig te identificeren, te beoordelen en aantoonbaar te beheersen. Dit risicomanagement wordt integraal uitgevoerd: fysieke beveiligingsrisico's worden niet los gezien, maar in samenhang met fysieke veiligheid van personen, informatiebeveiliging, beveiliging van procesautomatisering, cyberveiligheid en weerbaarheid.

4.6 Auditeerbaarheid

Voor alle wettelijke verplichtingen en interne normering geldt dat maatregelen aantoonbaar zijn. Dit betekent dat de organisatie beschikt over:

- actuele risicobeoordelingen,
- een maatregelenplan met prioriteit/eigenaar/termijnen,
- registraties van toegangsbeheer, onderhoud, testen, incidenten en opvolging,
- bestuurlijke besluitvorming over restrisico's en afwijkingen.

4.7 Continu verbeteren via vaste cyclus van beoordelen–toetsen–verbeteren

Het beleid en de uitvoering worden continu verbeterd via een vaste cyclus: beoordelen (risico's, incidenten, veranderingen), toetsen (audits, controles, oefeningen, KPI's) en verbeteren (maatregelen aanpassen, processen aanscherpen, lessen borgen). Hierdoor blijft de beveiliging passend bij veranderende dreigingen, organisatieontwikkelingen en technologische ontwikkelingen.

5 Governance en verantwoordelijkheden

De governance voor fysieke beveiliging is ingericht om eenduidige sturing, aantoonbaarheid en continue verbetering te borgen. Daarbij is de organisatie ingericht volgens het drie lijnen model, met heldere rollen voor uitvoering, kaderstelling/toezicht en onafhankelijke toetsing. Bestuurlijke verankering zorgt dat keuzes over risico's, middelen en restrisico expliciet en aantoonbaar worden gemaakt.

5.1 Bestuurlijke verankering

De eindverantwoordelijkheid voor fysieke beveiliging ligt bij de top van de organisatie. Binnen het waterschap is de bestuurlijke verankering als volgt ingericht:

5.1.1 Het Bestuur

Het bestuur is eindverantwoordelijk voor het stelsel van fysieke beveiliging en:

- stelt het bestuurlijk beleidskader fysieke beveiliging vast en bepaalt de risicobereidheid (risicoacceptatie en ambitieniveau);
- maakt middelen vrij (financieel en organisatorisch) voor de inrichting, instandhouding en verbetering van fysieke beveiliging;
- neemt besluiten over acceptatie van restrisico's wanneer risico's, ondanks maatregelen, niet verder (kosteneffectief) kunnen worden gereduceerd.

Hiermee is fysieke beveiliging bestuurlijk geborgd: het bestuur bepaalt de kaders en faciliteert,

5.2 Ambtelijke organisatie

5.2.1 De Directie

De directie is verantwoordelijk voor de vertaling van het beleidskader naar uitvoering en borging in de organisatie en:

- borgt dat fysieke beveiliging integraal onderdeel is van het assetmanagementproces, inclusief planvorming, ontwerp, realisatie, beheer, onderhoud en vervanging;
- zorgt dat risico's en maatregelen aantoonbaar worden meegenomen in lifecycle-besluiten, investeringsafwegingen en wijzigingsprocessen;
- stuurt op samenhang tussen fysieke beveiliging en aanpalende domeinen (o.a. informatiebeveiliging, crisisorganisatie, HR, facilitair, en leveranciersmanagement) zodat fysieke beveiliging structureel onderdeel is van de bedrijfsvoering en weerbaarheid.

Daarmee zorgt de directie zorgt voor integrale implementatie en verankering in het dagelijkse werk en het assetmanagement.

5.2.2 Eerste lijn – uitvoering en beheer

De eerste lijn is verantwoordelijk voor de dagelijkse uitvoering van fysieke beveiliging en het functioneren van de maatregelen in de praktijk. Hieronder valt:

- Operationele implementatie, werking en beheer van beveiligingsmaatregelen (preventie, detectie, respons).
- Toegangsbeheer in de dagelijkse praktijk (uitgifte, intrekking, mutaties, toepassing van procedures).
- Uitvoering van controles (rondes, verificaties, basischecks) en het vastleggen van bevindingen.

- Incidentopvolging (registratie, eerste beoordeling, herstelmaatregelen, escalatie).
- Leverancierssturing op afgesproken prestaties (onderhoud, storingsopvolging, alarmopvolging, SLA's).

5.2.3 Tweede lijn – kaderstelling, toezicht en coördinatie

De tweede lijn stelt de kaders en ziet toe op de werking daarvan. Deze lijn borgt dat fysieke beveiliging risico gestuurd, proportioneel en herleidbaar is en integraal wordt afgestemd met andere domeinen. Taken zijn onder meer:

- Opstellen en onderhouden van beleid, normering en minimale eisen (incl. zonering en toegangsprincipes).
- Risicosturing: faciliteren/uitvoeren van integrale risicoanalyses en bewaken van restrisico en acceptatie.
- Monitoring van prestaties en naleving (KPI's, trendanalyse, log- en rechtenreviews) en periodieke rapportage.
- Integrale afstemming met informatiebeveiliging, crisisorganisatie, HR en assetmanagement.
- Wwke-coördinatie: borgen van Wwke-proof procesinrichting, waaronder meldprocessen, documentatie-eisen en het opbouwen/onderhouden van een toetsbare audittrail.

De **Physical Security Officer** vervult een centrale rol in de tweede lijn en is verantwoordelijk voor:

- Kaderstelling en normering, toezicht op implementatie en werking, en integrale coördinatie.
- Regie op verbetercyclus, monitoring en rapportage.
- Coördinatie van Wwke-gerelateerde inrichting, meldprocessen en aantoonbaarheid.

Escalatiebevoegdheid: bij acute of onacceptabele risico's kan de Physical Security Officer direct escaleren richting directie/bestuur en tijdelijke beheersmaatregelen afdwingen (bijv. toegangsbeperking, extra toezicht, tijdelijke sluiting van een ruimte).

5.2.4 Derde lijn – stelselverantwoordelijkheid

De derde lijn voert onafhankelijke toetsen uit op de opzet, werking en naleving van het stelsel:

- Audits en reviews op governance, beheersmaatregelen en processen.
- Toetsing op effectiviteit (werkt het in de praktijk) en compliance (voldoet het aan kaders en eisen).
- Rapportage van bevindingen en opvolging via verbeteracties.

6 Thema’s 2026 – 20230

Governance, sturing en verantwoording (in control)

- Inrichten en versterken van de governance voor fysieke beveiliging, inclusief eenduidige rolverdeling, bevoegdheden, escalatie en besluitvorming.
- Realiseren van structurele sturing en verantwoording: periodieke rapportage, besluitvorming over restrisico’s en prioriteiten, aantoonbare opvolging van acties.
- Inrichten van toezicht (tweede lijn) en onafhankelijke assurance (derde lijn) met een vast ritme van toetsing en opvolging.

Periodieke risicobeoordeling en dreigingsbeeld (all hazards)

- Completeren en actueel houden van het fysieke dreigingsbeeld voor alle relevante dreigingen die essentiële dienstverlening kunnen verstoren.
- Borgen van een periodieke risicobeoordeling (all hazards), inclusief triggers voor tussentijdse actualisatie.
- Koppelen van risico’s aan concrete prioriteiten en maatregelen (audit trail: risico → maatregel → eigenaar → termijn → bewijs).

Classificatie en doelniveaus: normering die afdwingbaar is

- Actualiseren en borgen van classificatie van assets, processen en (waar relevant) personen, met herclassificatie bij wijzigingen.
- Vaststellen en onderhouden van beveiligingsniveau per locatietype en kritikaliteit, als basis voor de zorgplicht.
- Zorgen dat normering aantoonbaar wordt toegepast (acceptatiecriteria, controles, afwijkingsprocedure).

Zorgplicht: programma implementatie fysieke beveiligingsmaatregelen

- Opzetten van een meerjarig programma dat de kloof sluit tussen vastgesteld beveiligingsniveau en feitelijke situatie per asset.
- Prioriteren op basis van vitale processen en impact op essentiële dienstverlening.
- Vertalen van beveiligingsmaatregelen naar uitvoerbare projecten met eigenaarschap, budget, planning en bewijsvoering.

Meldplicht, incidentrespons en verslaglegging (operationeel en geoefend)

- Inrichten en borgen van meldproces voor incidenten die essentiële dienstverlening verstoren of kunnen verstoren.
- Inrichten van end-to-end incidentdossieropbouw inclusief tijdige oplevering van het gedetailleerde incidentverslag.
- Periodiek oefenen met escalatie, besluitvorming, communicatie en samenwerking met crisisorganisatie en informatiebeveiliging.

Uitvoering, capaciteit en expertise (doorpakken en leverkracht)

- Doorbreken van versnippering in de eerste lijn door centrale regie op uitvoering, prioritering en standaardisatie.
- Borgen van voldoende kennis, capaciteit en externe expertise om projecten en beheer structureel uit te voeren.
- Inrichten van een leveringsmodel (portfolio, ketenpartners, raamcontracten, projectherstart) dat stagnatie voorkomt.

Security-by-design in nieuwbouw, renovatie en veranderingen (hard gate)

- Verplichten van classificatie en beveiligingseisen in de initiatiefase van projecten en wijzigingen.
- Opnemen van fysieke beveiligingseisen in projectopdrachten, contracten en acceptatiecriteria.
- Formeel “go/no-go” mechanisme: geen voortgang naar ontwerp/uitvoering zonder aantoonbare inbedding van beveiliging.

Aantoonbaarheid, audittrail en onafhankelijke toetsing

- Inrichten van een “single source of truth” voor status fysieke beveiliging: maatregelenregister, assetstatus, incidenten, tests, audits, afwijkingen en risicoacceptaties.
- Periodieke interne controles en onafhankelijke audits op werking, met sluitende opvolging van bevindingen.
- Bestuurlijke rapportage over prestaties (KPI’s), risico’s (KRI’s) en verbeterprogramma’s.

Splitsing en invlechting van fysieke beveiliging (Waternet → AGV)

- Realiseren van een gecontroleerde invlechting van fysieke beveiliging vanuit de Gemeenschappelijke Dienst van Waternet naar AGV, zodat vitale beveiligingsprocessen, systemen en dienstverlening aantoonbaar continueren zonder verlies van sturing, compliance of operationele beschikbaarheid.
- Overzetten en inrichten binnen AGV van de kernfuncties:
    1. beveiligingsdienstverlening (objectbeveiliging, surveillance, meldkamer/security center waar van toepassing),
    2. toegangsmiddelenbeheer (passen, sleutels, certificaten/credentials waar relevant voor fysieke toegang),
    3. functioneel beheer (toegangscontrole/CCTV/alarmprocessen en gebruikersbeheer),
    4. contractmanagement beveiligingsdiensten (SLA’s, opvolging, prestatiemeting, escalatie),
    5. technisch applicatiebeheer van beveiligingssystemen (technische configuratie, onderhoud, patching/updates waar van toepassing, lifecycle en leverancierssturing).
- Borgen dat de invlechting integraal onderdeel is van governance, risicosturing en audittrail (rollen, bevoegdheden, registraties, bewijsvoering).
- Minimaliseren van transitierisico’s door een gefaseerde migratie met parallelle waarborgen, acceptatiecriteria en fallback-scenario’s.

7 Geldigheid en bijstelling

Dit Bestuurlijk beleidskader geldt voor 2026 – 2030 en wordt minimaal jaarlijks geëvalueerd en bijgesteld bij relevante wijzigingen in dreiging, assets, organisatie, incidenten en wetgeving. De evaluatie resulteert in een geactualiseerde roadmap en prioriteiten, inclusief bestuurlijke besluitvorming over restrisico's en investeringen.