

Onderwerp **Bestuurlijk Beleidskader fysieke beveiliging 2026-2030**

Case-nummer BBV26.0125

Portefeuillehouder Simon Deurloo / Sander Mager

Contactpersoon en contactgegevens Norbert de Blaay

Afdelingshoofd of programmamanager Sofie Gale

Inhoudelijk besluit Het Dagelijks bestuur besluit:

1. In te stemmen met het bestuurlijk beleidskader met de vijf leidende principes voor de fysieke veiligheid en deze ter vaststelling aan het Algemeen bestuur aan te bieden;
2. In te stemmen met het voorstel aan het Algemeen bestuur om de assets van AGV, conform de nieuwe Wet weerbaarheid kritieke entiteiten (Wwke) en de Cyberbeveiligingswet (CBW) in te richten, en daarvoor in de Voorjaarsnota 2027 een krediet van € 7,5 mln. voor de eerste fase op te nemen;
3. De ambtelijke organisatie de opdracht te geven om de organisatorische consequenties verder uit te werken en de financiële consequenties mee te nemen in het voorstel voor de Begroting 2027.

Het Algemeen bestuur besluit:

1. Het bestuurlijk beleidskader met de vijf leidende principes voor de fysieke veiligheid vast te stellen;
2. Om de assets van AGV, conform de nieuwe Wet weerbaarheid kritieke entiteiten (Wwke) en de Cyberbeveiligingswet (CBW) in te richten, en daarvoor in de Voorjaarsnota 2027 een krediet van € 7,5 mln. voor de eerste fase op te nemen.

Proces besluit Het Dagelijks bestuur

- ☒ stemt in met dit voorstel.
- ☒ verzendt dit voorstel naar de Commissie voor *oordeelsvorming*
- ☒ verzendt dit voorstel naar het Algemeen bestuur voor *besluitvorming*.

De Commissie

☒ adviseert over dit voorstel. Het Dagelijks bestuur stelt de volgende adviesvraag:
- Kan de commissie zich vinden in de vijf leidende beleidsprincipes (veiligheid van personen en continuïteit van dienstverlening staat voorop; risicogestuurd /proportioneel/herleidbaar; preventie–detectie–respons; laag-op-laag; strikt toegangsbeheer) als basis voor normering, maatregelkeuze en acceptatie van restrisico's?

Het Algemeen bestuur

☒ stelt dit voorstel vast

Planning BOB	DB	Datum vergadering	AB	Datum
	vergadering			
	Beeldvorming	→	Beeldvorming	
	↓		↓	
	Oordeelsvorming	→	Oordeelsvorming Commissie	26/03/2026
	↓		↓	
	Besluitvorming	10/03/2026	Besluitvorming AB	16/04/2026

Kernboodschap t.b.v. de Aanleiding
besluitenlijst (max. 100 woorden)

Bestuursvoorstel

Naar verwachting wordt AGV in Q2 van dit jaar aangewezen als kritieke entiteit, zodra de Wet weerbaarheid kritieke entiteiten (Wwke) in werking treedt. Om invulling te geven aan deze nieuwe wetgeving is een nieuw fysiek beveiligingsbeleid voor AGV opgesteld.

Bestuurlijke duiding

De ontwikkelingen in wetgeving vergen een versterking van de beveiliging binnen het waterschap en de betrokkenheid van het bestuur daarbij. Er komen nieuwe verplichtingen op ons af. Er worden hogere veiligheidseisen gesteld aan de assets, de organisatorische processen en de organisatie.

Fysieke beveiliging is randvoorwaardelijk voor de continuïteit en veiligheid van de essentiële waterschapstaken (waterkeringen, peilbeheer, afvalwaterzuivering). Met de keuze voor de vijf leidende principes geeft het bestuur richting in de wijze waarop fysieke beveiliging wordt ingericht.

Genomen besluit

Het bestuur stelt het Bestuurlijk Beleidskader Fysieke Beveiliging 2026–2030 vast en besluit een krediet van € 7,5 mln. voor de eerste fase op te laten nemen in het voorstel voor de Voorjaarsnota 2027-2031.

Bespreking <‘op basis van de commissiebespreking is het voorstel aangepast op het volgende:...' of ' op in CIE basis van de commissiebespreking heeft geen aanpassing op het voorstel plaatsgevonden'>

Bijlagen Bijlage 1: Bestuurlijk Beleidskader Fysieke Beveiliging 2026-2030
Bijlage 2: AB-besluit 16-04-2026

1. ARGUMENTEN EN ALTERNATIEVEN

1.1 Probleemanalyse AGV levert essentiële diensten (o.a. waterkeringen, peilbeheer en afvalwaterzuivering) die ook onder versturende omstandigheden moeten blijven functioneren. Fysieke dreigingen zoals inbraak, sabotage, vandalisme, diefstal, intimidatie en brandstichting kunnen de continuïteit van deze dienstverlening direct aantasten. Daarnaast kunnen fysieke incidenten ook doorwerken naar procesautomatisering en informatiesystemen; fysieke en digitale weerbaarheid zijn daarom in de praktijk onlosmakelijk verbonden.

De afgelopen jaren is gewerkt om alle assets te voorzien van adequate fysieke beveiligingsmaatregelen volgens de wettelijke Baseline Informatiebeveiliging Overheid (BIO) en CyberSecurity ImplementatieRichtlijn (Csir). Vanuit een huidig krediet worden dit jaar de laatste prioritaire assets voorzien van fysieke beveiligingsmaatregelen. Dit betreft vijf hoge prioriteit assets (poldergemalen) vanuit het effect voldoende water en twee zuiveringslocaties (Amstelveen en deels Horstermeer) vanuit het effect gezuiverd water. Hiermee zijn de assets met de hoogste risico's voorzien van fysieke beveiliging (40%) wat rest vanuit het eerdere krediet zijn assets met een lagere prioriteit vanuit de BIO en Csir.

Naar verwachting treedt de Wet weerbaarheid kritieke entiteiten (Wwke) in Q2 van 2026 in werking. De waterschappen wordt daarmee aangewezen als kritieke entiteiten. Dit brengt voor AGV (en voor alle waterschappen) verplichtingen met zich mee rond o.a. periodieke risicobeoordeling (all hazards), zorgplicht (passende en evenredige maatregelen), incidentmelding/ verslaglegging en aantoonbaar “in control” zijn.

1.2 Argumenten gekozen oplossing of antwoord De nieuwe wetgeving is vertaald in een nieuw fysiek beveiligingsbeleid. Hiermee worden bestuurlijke kaders gesteld voor het uitvoeren van fysieke beveiligingsmaatregelen van AGV-assets.

De voorgestelde vijf leidende principes van het beleidskader zijn:

1. Veiligheid van personen en continuïteit van dienstverlening staat voorop;
2. Risicogestuurd, proportioneel en herleidbaar (maatregelkeuze en restrisico);
3. Preventie is de basis, detectie en respons sluiten hierop aan;

Bestuursvoorstel

4. Laag-op-laag beveiliging (perimeter–gebouw–kritieke ruimte–kritieke asset);
5. Strikt toegangsbeheer (uitgifte, intrekking, review, logging)

Het beleidskader borgt een integrale aanpak (afstemming met o.a. risicomanagement, informatiebeveiliging en crisisorganisatie) omdat fysieke toegang direct invloed heeft op IT/OT-risico's. En het beleidskader legt de basis voor auditbaarheid: actuele risicobeoordelingen, maatregelenplan met eigenaar/termijnen en registraties van toegangsbeheer, onderhoud, testen, incidenten en opvolging. Ook verankert het beleidskader de governance (drie-lijnenmodel) en maakt sturing en verantwoording structureel, incl. escalatie bij acute/onacceptabele risico's.

Bij het in kaart brengen van de organisatorische consequenties van het beleid voor AGV kunnen mogelijk nog dilemma's naar voren komen. Indien daar sprake van is, worden deze ook voor het Algemeen bestuur inzichtelijk gemaakt.

1.3 Alternatieve oplossingen of antwoorden

Alternatief A – Geen bestuurlijk beleidskader, alleen operationele maatregelen per locatie/project

- **Voor:** sneller “klein beginnen”; minder bestuurlijke besluitvorming.
- **Tegen:** vergroot versnippering; maakt herleidbaarheid/audittrail lastiger en belemmert uniforme sturing en aantoonbaarheid richting toezicht.

Alternatief B – Uitstellen tot na aanwijzing als kritieke entiteit / na ontvlechting Waternet

- **Voor:** mogelijk meer duidelijkheid over definitieve eisen/overdracht.
- **Tegen:** verkleint voorbereidingstijd voor wettelijke termijnen (risicobeoordeling/maatregelen/incidentprocessen) en vergroot transitierisico's bij overname van vitale beveiligingsfuncties.

Alternatief C – Beperk scope tot “minimale compliance” (alleen Wwke-eisen) zonder brede governance/verbetercyclus

- **Voor:** beperkt inspanning op korte termijn.
- **Tegen:** mist structurele verbetercyclus en audit-ready inrichting (registraties, monitoring, onafhankelijke toetsing) en borgt weerbaarheid minder duurzaam.

1.4 Gevolgen niet instemmen

Bij niet-instemmen ontbreekt een bestuurlijk vastgesteld kader voor fysieke beveiliging, terwijl AGV als (aanstaande) kritieke entiteit verplicht wordt om o.a. risicobeoordeling, passende maatregelen, incidentmelding/verslaglegging en aantoonbare “in control” inrichting te realiseren. Dit vergroot het risico op non-compliance en onvoldoende auditbaarheid. En mogelijk vergroot het de kans op incidenten. De Wet weerbaarheid kritieke entiteiten biedt de mogelijkheid om bestuurders van kritieke entiteiten in een uiterst geval aansprakelijk te stellen.

2. POLITIEK - BESTUURLIJKE CONTEXT

2.1 Eerder vastgestelde kaders In 2019 heeft het bestuur van AGV een krediet toegekend (BBV19.0182) om een start te maken met de implementatie van fysieke beveiligingsmaatregelen op hoog risico-assets. Over de kredietaanvraag fysieke beveiligingsmaatregelen deel 2 is door het DB besloten in 2020 (BBV20.0420).

2.2 Bestuurlijke thema's

Klimaat: Dit voorstel heeft vooral een randvoorwaardelijke impact: het beschermt vitale assets en processen die nodig zijn om de (primaire) waterschapstaken betrouwbaar te blijven uitvoeren, ook bij fysieke verstoringen.

Digitalisering: er is een directe koppeling, omdat fysieke toegang en fysieke incidenten impact kunnen hebben op procesautomatisering en informatiesystemen; daarom is integrale afstemming met informatiebeveiliging expliciet onderdeel van het kader.

Bestuursvoorstel

2.3 Effectsturing ERAM	Het besluit draagt bij aan het effect Voldoende- en Gezuiverd afvalwater. Het verbeteren van de fysieke beveiliging assets betreft het technische areaal binnen het watersysteem (sluizen, bruggen, poldergemalen), rioolgemalen en rioolwaterzuiveringen.
2.4 Rol en verantwoordelijkheid AGV	AGV is verantwoordelijk voor het borgen van continuïteit van essentiële dienstverlening en voor het voldoen aan de (aanstaande) wettelijke verplichtingen rond fysieke weerbaarheid.
2.5 Informeren bestuur	Het bestuur wordt over de voortgang van dit voorstel geïnformeerd via de rapportage grote projecten.

3. OMGEVING

3.1 Stakeholderanalyse externe belangen en participatieplan	Voor AGV zijn de volgende stakeholders van belang: • NCTV heeft een coördinerende rol rond vitale infrastructuur en de Wwke; • Ministerie van IenW is verantwoordelijk voor de toepassing van de Wwke binnen hun sector (kaders, sectorale invulling, ondersteuning), afhankelijk van sectorindeling kan het ministerie van EZ een rol hebben bij aanwijzing/afbakening; • Veiligheidsregio / crisispartners: Fysieke weerbaarheid raakt crisisbeheersing (rampen, sabotage, verstoringen); • Politie en Openbaar Ministerie: Bij fysieke beveiliging (inbraak, vernieling, sabotage) zijn opsporing/handhaving relevante stakeholders; • Inlichtingen- en veiligheidsdiensten: dreigingsinformatie rond statelijke dreigingen/sabotage; • Gemeenten en Provincies: Assets liggen in hun gebied; vergunningen/handhaving (bouwen, natuur, camera's), ruimtelijke inpassing en maatschappelijke impact; • Omgevingsdiensten: Voor aanpassingen aan hekwerken, verlichting, toegangssystemen, camera's of bouwwerken. • Waternet (Gemeenschappelijke Dienst): overdracht/invlechting van vitale beveiligingsfuncties, systemen en dienstverlening. • Leveranciers / beveiligingsdienstverleners: prestaties op onderhoud, storings- en alarmopvolging, SLA's en leverancierssturing. • Publieke veiligheidspartners/ketenpartners (crisis/veiligheid): samenwerking is onderdeel van aanpalende crisis- en veiligheidswetgeving
3.2 Stakeholderanalyse belangen binnen de organisatie	Verschillende afdelingen zijn betrokken bij de vormgeving van de fysieke beveiliging. Het maakt onderdeel van de reguliere processen waarbij deze afdelingen de volgende belangen hebben: • 1e/2e/3e lijn (drie-lijnenmodel): uitvoering & beheer, kaderstelling/toezicht (incl. Physical Security Officer) en onafhankelijke toetsing/audit. • Afdeling assetmanagement en afdeling projecten (nieuwbouw/renovatie/wijzigingen): security-by-design en "go/no-go" mechanisme zodat projecten niet door kunnen zonder aantoonbare inbedding van beveiligingseisen. • Informatiebeveiliging (IT/OT) en procesautomatisering: integrale afstemming omdat fysieke beveiliging direct effect heeft op cyber- en OT-risico's. • Crisisorganisatie: oefenen met escalatie/besluitvorming/communicatie en incidentrespons voor de fysieke dreigingen. • Facilitair / leveranciersmanagement: samenhang van fysieke beveiligingsdienstverlening borgen in bedrijfsvoering en duidelijke rol-/overdrachtsmomenten.
3.3 Publiciteit en communicatie	Dit betreft primair een intern sturings- en compliance kader. Communicatie kan intern worden ingezet voor bewustwording, heldere werkwijzen rond toegangsbeheer en incidentmelding (rollen, registratie, kwaliteitscontrole) en voor het borgen van "audit-ready" werken.

Bestuursvoorstel

4. JURIDISCHE KADERS

4.1 Wettelijke taken en/of juridische verplichtingen

De fysieke beveiliging sluit aan op en ondersteunt o.a.:

- Wwke (risicobeoordeling, zorgplicht, incidentmelding/verslaglegging, toezicht/auditbaarheid) en het Besluit weerbaarheid kritieke entiteiten.
- Cyberbeveiligingswet (bestuurlijke verantwoordelijkheid, zorgplicht, meldplicht, toezicht/auditbaarheid) voor samenhang fysiek–digitaal.
- Arbowetgeving (veilige werkomgeving; beheersing agressie/geweld; veilige processen voor medewerkers/contractors).
- AVG (cameratoezicht, logging, doelbinding, rechten, bewaartermijnen en DPIA's waar nodig).
- Archiefwet (bewaarplichten voor registraties, besluitvorming en incidentdossiers).

4.2 Bevoegdheid besluit

Het Algemeen bestuur stelt de vijf leidende principes als kader voor de fysieke beveiliging van AGV vast. De uitvoering is aan de directie.

4.3 Ter inzagelegging

Niet van toepassing bij vaststelling van een intern beleidskader.

5. RISICO'S EN BEHEERMAATREGELEN

Risico 1

Het programma Fysieke Beveiliging heeft veel uitwerking en vertaling nodig, daarnaast is het intensief om relatief kleine maatregelen uit te rollen bij alle assets. Dit kost tijd en we hebben te maken met tekort aan mensen en afhankelijkheid van meerdere teams en leveranciers.

De uitvoering loopt vertraging op doordat interne capaciteit (ontwerp, besluitvorming, uitvoering, beheer) of externe capaciteit (leveranciers, monteurs) niet beschikbaar is wanneer nodig.

Beheermaatregel 1

Eén integraal plan: wie doet wat, wanneer, met welke capaciteit (intern én extern).

Werken met standaard “werkpakketten” zodat uitvoering herhaalbaar is en minder afstemming vraagt per locatie.

We prioriteren met het uitvoeren van de maatregelen. Hierbij starten met de assets met grootste impact. Waar nodig huren we extra capaciteit in.

Inrichten van een stuurgroep die knopen doorhakt bij afhankelijkheden en planningsconflicten.

Capaciteit voor een langere periode vastleggen om wisselingen en afstemmingsproblemen te beperken.

Risico 2

Onvoldoende auditbaarheid / niet “in control” richting toezicht

Omschrijving: ontbrekende/versnipperde bewijsvoering (risicobeoordeling, maatregelenplan, registraties, incidentdossiers) waardoor compliance en toetsbaarheid onder druk komen.

Beheermaatregel 2

“single source of truth” (maatregelenregister, assetstatus, incidenten, tests, audits, afwijkingen, risicoacceptaties) + periodieke interne controles en onafhankelijke audits met sluitende opvolging.

Risico 3

Onvoldoende uitvoeringskracht/capaciteit (stagnatie implementatie zorgplicht)

Bestuursvoorstel

Omschrijving: onvoldoende kennis/capaciteit of versnipperde uitvoering leidt tot vertraging bij het dichten van de kloof tussen vastgesteld beveiligingsniveau en feitelijke situatie per asset.

Beheermaatregel 3 Meerjarig programma met prioritering op vitale processen/impact, centraal regiemodel en ingericht leveringsmodel (portfolio/raamcontracten) om stagnatie te voorkomen.

6. FINANCIËLE KADERS

6.1 Kostenraming Er zijn geen kosten verbonden aan vaststelling van het fysieke beveiligingsbeleid, maar wel aan de uitvoering daarvan. In de Voorjaarsnota 2027-2031 wordt een nieuw krediet voorgesteld aan het AB voor de 1ste fase van de maatregelen fysieke beveiliging.

Met dit krediet wordt begonnen met de assets die het hoogste risico vormen vanuit de nieuwe Wwke en/of waar een groot effect is op het functioneren van onze assets. De investeringskosten gedurende de looptijd van het fase 1 krediet bedragen naar verwachting € 7,5 mln. waarvan € 3,1 mln. ten laste van het effect gezuiverd afvalwater (BBP13) en € 4,4 mln. ten laste van het effect voldoende water (BBP09). Onderdeel van fase 1 is het in beeld brengen van de totale investering waarmee een krediet voor fase 2 zal worden aangevraagd. De totale investeringskosten (fase 1 en fase 2) worden op basis van de huidige informatie ingeschat op € 17,5 mln. In 2026 wordt het nieuwe beleid uitgewerkt naar concrete maatregelen per assetgroep. Zodra de te nemen maatregelen beter in beeld zijn kunnen we de impact bepalen en de realisatie prioriteren.

In fase 2 zijn alle maatregelen in beeld en zullen de resterende assets worden voorzien van fysieke beveiliging volgens de Wwke. Daarnaast naderen veel van de beveiligingsmaatregelen vanuit eerdere investeringen tegen die tijd hun einde technische levensduur en zullen moeten worden vervangen.

6.2 Voorjaarsnota en begroting De uitvoering vraagt om bestuurlijke besluitvorming over investeringen en middelen (financieel en organisatorisch) en periodieke bijstelling van roadmap/prioriteiten. In de Voorjaarsnota 2027 wordt voor het versterken van de fysieke beveiliging van de kritieke infrastructuur een krediet opgenomen. De financiële consequenties voor de organisatie worden voor de begroting 2027 uitgewerkt.

6.3 Subsidieaanvraag AGV onderzoekt of (en zo ja onder welke voorwaarden) het waterschap in aanmerking kan komen voor een EU subsidie (Internal Security Fund (counter terrorisme) (ISF) en/of deelname passend is bij de beoogde maatregelen en planning. De subsidie bevat onder meer de onderwerpen versterking van het CER-kader en sector overstijgende/grensoverschrijdende stresstesten voor de weerbaarheid van kritieke infrastructuur. Indien het onderzoek positief uitvalt, wordt een eventuele subsidieaanvraag voorbereid.

6.4 Aanvullende financiering n.v.t.

6.5 Fiscale aspecten n.v.t.