Nijmegen

Postadres
Gemeente Nijmegen
Postbus 9105
6500 HG Nijmegen

Bezoekadres
Korte Nieuwstraat 6
6511 PP Nijmegen

T 14 024
nijmegen.nl

Contactgegevens
nijmegen.nl/contact

Ons kenmerk
E25.002485

Bijlage(n)
Bijgevoegd: Ja

Aan de gemeenteraad van Nijmegen

Datum 16 december 2025
Onderwerp Rapportage 213a doelmatigheidsonderzoek fysieke toegang en beveiliging

Geachte leden van de raad,

Inwoners moeten erop kunnen vertrouwen dat de gemeente effectief, efficiënt, transparant en integer met gemeenschapsgeld omgaat. Op grond van artikel 213a van de Gemeentewet zijn gemeenten verplicht om zelf onderzoek te doen naar de doelmatigheid en doeltreffendheid van het door het college gevoerde bestuur.
Deze onderzoeken bieden niet alleen inzicht in hoe middelen worden ingezet, maar dragen ook bij aan transparantie en vertrouwen richting inwoners.

In de Stadsbegroting 2025 is aangekondigd dat in 2025 een doelmatigheidsonderzoek wordt uitgevoerd naar de fysieke toegang en beveiliging van onze kantoorgebouwen. Doelmatigheid gaat over het bereiken van maximale prestaties met minimale middelen, of het verbeteren van kwaliteit zonder extra kosten.

Het doel van fysieke toegang en beveiliging is meerledig:

- het beperken van toegang tot gevoelige informatie, hardware en IT-systemen tot geautoriseerd personeel;
- het verkleinen van risico's op inbraak en diefstal door middel van maatregelen zoals alarmsystemen, bewakingscamera's en beveiligingspersoneel.

Het onderzoek richt zich op de locaties Mariënburg, Stadhuis en het Regionaal Archief Nijmegen (RAN). Het gaat dan met name om de beveiligde zones van deze gebouwen, waar over het algemeen met gevoelige informatie wordt gewerkt. Een beveiligde zone wil zeggen dat toegang uitsluitend kan worden verkregen met een medewerker- of bezoekerspas. Hiervoor is de periode vanaf de invoering van de toegangspoortjes in het Stadhuis en de Mariënburg op 1 oktober 2021 tot heden onderzocht. Deze poortjes zijn In het kader van fysieke toegang en beveiliging geplaatst. Daarnaast heeft Facilitaire Zaken het toegangsbeleid opgesteld respectievelijk geactualiseerd voor medewerkers, bezoekers en leveranciers. De Baseline Informatiebeveiliging Overheid (BIO)[1] beschrijft de eisen voor

[1] Baseline Informatiebeveiliging Overheid - het basisnormenkader voor informatiebeveiliging binnen alle overheidslagen

inrichting en implementatie van fysieke beveiligingsmaatregelen en vormt de basis van dit beleid.

Belangrijkste uitkomsten
Het beleid voor fysieke toegang en beveiliging is in de kern doelmatig. Met redelijke middelen wordt een goed basisniveau van fysieke toegang beveiliging bereikt dat vergelijkbaar is met dat van drie andere G40 - gemeenten. De belangrijkste voorzieningen en maatregelen, zoals poortjes, paslezers, bezoekersregistratie en alarm, functioneren naar behoren. Ook het intrekken van toegangsrechten bij uitdiensttreding of het beëindigen van werkzaamheden verloopt efficiënt. Aanvullende maatregelen binnen afdelingen worden risico-gebaseerd getroffen. Met de huidige inrichting voldoen wij grotendeels aan onze eigen ambitie om minimaal te voldoen aan de BIO-norm.

Tegelijkertijd blijkt uit de bevindingen dat met relatief beperkte inspanningen en enkele quick wins een hoger beveiligingsniveau kan worden bereikt. Dagelijkse incidenten, zoals ongeautoriseerd meelopen door de poortjes, onvolledige bezoekersregistratie en het niet terugbegeleiden van bezoekers leiden tot risico's en extra werk voor de receptie. Een recent incident waarbij een inwoner driemaal onbevoegd toegang kreeg tot de beveiligde zone van een kantoorgebouw, laat zien dat we ondanks de huidige maatregelen kwetsbaar blijven. Hoewel er in het verleden geen vergelijkbare incidenten zijn gemeld, blijft dit een reëel risico. Dat incidenten niet bekend zijn, betekent immers niet dat ze niet voorkomen. Zo zijn in het verleden niet alle incidenten geregistreerd. Ook het mystery-guest onderzoek uit 2022 laat zien dat onbevoegden nauwelijks worden herkend of aangesproken.

De effectiviteit van de poortjes hangt dus sterk af van het gedrag van medewerkers. Het gebruik van duidelijk onderscheidende toegangspassen voor medewerkers en bezoekers, en het zichtbaar dragen ervan, kan dit risico verkleinen. Daarnaast kan de werking van de poortjes eenvoudig worden verbeterd door de anti-pass-backfunctie te activeren, waardoor een pas niet meerdere keren kan worden gebruikt. Het gebruiksvriendelijker maken van de bezoekersregistratie vergroot bovendien naar verwachting de naleving daarvan. Ook het feit dat medewerkers buiten openingstijden toegang kunnen krijgen, kan leiden tot onnodige kosten door een onterecht alarm en inzet van beveiliging. Een goede onboarding en regelmatige communicatie over huisregels kunnen de effectiviteit van bestaande maatregelen tegen minimale extra kosten versterken.

Op langere termijn kunnen grotere aanpassingen de doelmatigheid verder verbeteren. Door toegangsrechten automatisch te koppelen aan iemands functie en deze automatisch te verwijderen bij een functiewijziging, vermindert het handmatige beheer en daarmee de kans op fouten. De overstap naar beter beveiligde toegangspassen of naar een app-gebaseerd toegangssysteem vraagt een grotere investering, maar verlaagt op termijn structureel het risico op misbruik.

Vervolg
Wij geven vervolg aan de aanbevelingen. Waar nodig worden deze verder uitgewerkt in een concreet plan.

Hoogachtend,

Het college van burgemeester en wethouders van Nijmegen

A.P.W. van de Klift
gemeentesecretaris

H.M.F. Bruls
burgemeester