DE HAAGSE HOGESCHOOL

VASTGESTELD BESLUIT DOOR HET COLLEGE VAN BESTUUR:

Onderwerp	**Protocol Cameratoezicht**
Besluit	Een veilige school is belangrijk voor De Haagse Hogeschool. Studenten, medewerkers en bezoekers moeten zich veilig voelen op school. Om bij te dragen aan dit veiligheidsgevoel maakt De Haagse Hogeschool gebruik van cameratoezicht. In dit protocol cameratoezicht wordt omschreven op welke wijze betrokkenen dienen om te gaan met camera's en camerabeelden. Dit protocol gaat in op taken, verantwoordelijkheden, bevoegdheden en procedures ten aanzien van cameratoezicht. Voorop staat dat integriteit in het omgaan met camerabeelden van groot belang is. De Haagse Hogeschool heeft dit protocol opgesteld met inachtneming van wet- en regelgeving betreffende cameratoezicht. Dit protocol cameratoezicht wordt tenminste eens per drie jaar herzien. Met dit protocol wordt voldaan aan de eis zorgvuldig om te gaan met het camerasysteem en eventuele uitbreiding of aanpassing ervan op een zorgvuldige manier te laten verlopen. Het CvB stelt het Protocol Cameratoezicht definitief vast na instemming van de Hogeschoolraad in de overlegvergadering d.d. 16 juli 2020. Het CvB heeft daarbij de vraag van de Hogeschoolraad opgevolgd en expliciet in het protocol opgenomen hetgeen de wet voorschrijft ten aanzien van de behandeling van geluidsopnames (algemeen en heimelijk toezicht).
Vastgesteld d.d.	25 augustus 2020

Protocol Cameratoezicht

Dienst FZ&IT

let's change
YOU. US. THE WORLD.

DE HAAGSE
HOGESCHOOL

Protocol Cameratoezicht

Dienst FZ&IT

Auteur
J.J.C. van Koppen
Adviseur Veiligheid en BHV

Afdeling
FZ&IT, Unit I&P, Team Veiligheid

Versie
1.0

Datum
21-7-2020

Datum vaststelling CvB
1-9-2020

Voorwoord

Een veilige school is belangrijk voor De Haagse Hogeschool. Studenten, medewerkers en bezoekers moeten zich veilig voelen op school. Om bij te dragen aan dit veiligheidsgevoel maakt De Haagse Hogeschool gebruik van cameratoezicht.

Cameratoezicht vormt een onderdeel van het veiligheidsconcept zoals dat binnen De Haagse Hogeschool bestaat. Het veiligheidsconcept van De Haagse Hogeschool omvat momenteel de volgende – in enkele gevallen overlappende – gebieden:

- Het voorkomen van schade aan het welzijn als ook de geestelijke- en lichamelijke gezondheid van medewerkers, studenten en betrokken derden ('fysieke veiligheid' / *'safety'*)
- Het tegengaan van slachtofferschap en onveiligheidsgevoelens ('sociale veiligheid') onder medewerkers, studenten en betrokken derden
- Het beschermen van (waardevolle) eigendommen ('assets') en informatie middels beveiliging ('security')
- Het bevorderen en bewaken van de integriteit van medewerkers, studenten en betrokken derden
- Het garanderen van de continuïteit van diensten die een veilige leer- en werkomgeving helpen mogelijk maken (*business continuity management*)
- Het beperken van schade aan merk en imago als gevolg van onveiligheid
- Het adequaat organiseren van incident- en crisismanagement om de effecten van acute onveiligheid zoveel mogelijk te reduceren

Cameratoezicht draagt bij aan de verwezenlijking van bovenstaande. In dit protocol cameratoezicht wordt omschreven op welke wijze betrokkenen dienen om te gaan met camera's en camerabeelden. Dit protocol gaat in op taken, verantwoordelijkheden, bevoegdheden en procedures ten aanzien van cameratoezicht. Voorop staat dat integriteit in het omgaan met camerabeelden van groot belang is. De Haagse Hogeschool heeft dit protocol opgesteld met inachtneming van wet- en regelgeving betreffende cameratoezicht.

Dit protocol cameratoezicht wordt tenminste eens per drie jaar herzien.

De Haagse Hogeschool

Den Haag, april 2020

1. Inleiding

Cameratoezicht biedt een organisatie handvatten om grip te krijgen op mogelijke risico's. Een organisatie kan verschillende redenen hebben om op cameratoezicht over te gaan. De plaatsing van camera's bij De Haagse Hogeschool leveren een bijdrage aan het verhogen van de veiligheid van studenten, medewerkers en bezoekers. Cameratoezicht wordt selectief ingezet onder zorgvuldige afweging van rechten en belangen.

Cameratoezicht is primair gekaderd in de privacywetgeving. De Algemene Verordening Gegevensbescherming (AVG) geeft wettelijke kaders aan met betrekking tot het verwerken van persoonsgegevens. De AVG geeft de noodzaak voor een goed protocol cameratoezicht aan. Het protocol cameratoezicht is gebaseerd op de geldende wettelijke bepalingen. Deze bepalingen zijn door de Autoriteit Persoonsgegevens (AP) uitgewerkt in een apart document, waarbij beleidsregels zijn opgesteld met betrekking tot cameratoezicht. Deze richtlijnen worden toegepast in het protocol cameratoezicht.

Cameratoezicht binnen De Haagse Hogeschool staat zoals eerder vermeld in een groter geheel aan maatregelen om veiligheid te waarborgen. In dit protocol wordt beschreven op welke wijze De Haagse Hogeschool inhoud geeft aan cameratoezicht. Het College van Bestuur (CvB) van De Haagse Hogeschool draagt de eindverantwoordelijkheid voor het cameratoezicht, de Directeur Facilitaire Zaken en Informatietechnologie (verder: Directeur FZ&IT) is verantwoordelijk voor de uitvoering en naleving van het protocol cameratoezicht. De Hogeschoolraad is gekend en stemde in (met) dit protocol.

2. Werkingssfeer en doelstelling cameratoezicht

2.1 Werkingssfeer

Dit reglement is van toepassing op studenten, medewerkers en bezoekers die zich bevinden in de gebouwen of op de terreinen van De Haagse Hogeschool.

Haagse Hogeschool-locaties

Dit Protocol is van toepassing op alle gebouwen en terreinen die De Haagse Hogeschool gebruikt voor haar bedrijfsvoering. Deze zijn:

1. Johanna Westerdijkplein 75, 2521 EN Den Haag (hierna benoemd als **Hoofdlocatie**)
2. Rotterdamseweg 137, 2628 AL Delft (hierna benoemd als locatie **Delft**)
3. Mr. P. Droogleever Fortuynweg 22, 2533 SR Den Haag (hierna benoemd als **Sportcampus**)
4. Bleiswijkseweg 37, 2712 PB Zoetermeer (hierna benoemd als locatie **Zoetermeer**)
5. Johanna Westerdijkplein 109, 2521 EN Den Haag (hierna benoemd als **Poseidon**)

In die gebouwen waarbij De Haagse Hogeschool medehuurder of –eigenaar is, heeft dit protocol enkel betrekking op die delen die toebehoren aan De Haagse Hogeschool.

2.2 Doelstelling

Cameratoezicht beoogt de volgende doelen:

- Het bevorderen van het veiligheidsgevoel van studenten, medewerkers en bezoekers;
- Het verminderen van schade door onveiligheid;
- Preventie van ongewenst gedrag t.o.v. medewerkers en studenten;
- De beveiliging van eigendommen;
- Het registreren en voorkomen van en anticiperen op incidenten;
- Het voorkomen van vandalisme;
- Het verminderen of voorkomen van criminele activiteiten;
- Het weren van overlast.
- Het bevorderen en ondersteunen van een veilig schoolklimaat
- Het bevorderen van opsporing en vervolging van strafbare feiten;

Voorafgaand aan de inzet van het cameratoezicht zoals omschreven in dit protocol is conform artikel 35 AVG een gegevensbeschermingseffectbeoordeling, ofwel *Data Protection Impact Assesment* (hierna: DPIA), uitgevoerd.

3. Plaats- en tijdsbepaling

Dit protocol geldt op alle locaties van De Haagse Hogeschool waar cameratoezicht plaatsvindt. De Haagse Hogeschool maakt 24 uur per dag opnames van eigen gebouwen, terreinen en ruimten. Het is geen taak voor De Haagse Hogeschool om toezicht te houden op het openbaar gebied. De posities van de camera's zijn ingericht om eigen terreinen en gebouwen te bewaken en er zijn technische maatregelen genomen om opnames van buiten het eigen terrein te beperken. Het cameratoezicht wordt kenbaar gemaakt bij de ingang(en) van het betreffende gebouw.
Expliciet omvat dit protocol niet het gebruik van camera's ten behoeve van onderwijs. Dergelijk gebruik van camera's is uiteraard ook aan regelgeving gebonden, maar wordt dus niet in dit protocol behandeld.
Bij de plaatsing van de huidige camera's zijn de volgende uitgangspunten gebruikt:

- Er dienen op alle entrees en nooduitgangen en op de hoofdentree camera's gericht te zijn. In de buitenschil dienen de camera's voor het overzicht op het terrein, op cruciale plekken worden zogenaamde *Pan-Tilt-Zoom* (PTZ)-camera's toegepast wat de beveiliging de mogelijkheid geeft om verdachte activiteiten nader te onderzoeken.
- Bij betreding van de locatie vanuit buiten kunnen identificatiecamera's worden opgesteld; deze camera's dienen om binnengaande personen eenmalig op hoge kwaliteit op opname te hebben, wat dient voor eventuele identificatie van personen op de vervolgbeelden, of om de hoeveelheid binnenkomers te tellen. Momenteel is er geen aanleiding om dit te doen; als de (veiligheids)situatie verandert wellicht wel.

Camera's worden in principe niet geplaatst op de volgende locatie:

- In (of primair gericht op) werkruimten van medewerkers

Camera's worden niet geplaatst op de volgende locaties:

- In (voorhallen van) toiletten
- In kleed- en doucheruimten
- In onderwijsruimten

In enkele gevallen is er een camera gericht op de primaire werkplek van een medewerker; de activiteiten bij de ingang van een pand en een balie worden namelijk door de camera gemonitord. Het is dan dus niet te vermijden dat de activiteiten van de medewerkers opgenomen worden. In deze situatie mag de medewerker verwachten dat hij/zij op de hoogte gebracht wordt van de camera en het bereik. Indien gewenst en mogelijk gezien de aard van de werkzaamheden kan de medewerker verwachten dat al het mogelijke wordt gedaan om bijvoorbeeld het scherm van de medewerker te maskeren.

Toelichting huidige weergaves per locatie:

Locatie	**Beeldweergave**	**Toegankelijk voor**
Johanna Westerdijkplein 75 2521 EN Den Haag (**Hoofdlocatie**)	Milestone (live+terugkijken)	-Beveiliging
	SMS (live+terugkijken)	-Beveiliging
	Video Wall (live)	-Iedereen, maar omdat het enkel live beelden betreft is dat geen probleem
Johanna Westerdijkplein 109 2521 EN Den Haag (**Poseidon**)	Milestone (alleen live van locatie)	Beveiliging + Receptiemedewerkers
Johanna Westerdijkplein 109 2521 EN Den Haag (**Poseidon**) Rotterdamseweg 13 2628 AL Delft (**Delft**)	Milestone (alleen live van locatie)	Beveiliging + Receptiemedewerkers
	Back-up Meldkamer Poseidon	Staat niet actief aan en kan alleen worden opgestart door aangewezen personen
Rotterdamseweg 13 2628 AL Delft (**Delft**) Mr. P. Droogleever Fortuynweg 22 2533 SR Den Haag (**Sportcampus**)	SMS (alleen live van locatie)	Beveiliging + Receptiemedewerkers
	Milestone, momenteel niet actief bekeken bij receptie	Beveiliging Hoofdlocatie kan beelden terugkijken
Bleiswijkseweg 37 2712 PB Zoetermeer (**Zoetermeer**)	Milestone (alleen live van locatie)	Beveiliging + Receptiemedewerkers

Camerabeelden worden op de eigen HHs-server (hhs-msa0001.ads.hhs.nl) opgeslagen, middels het door de technisch leverancier Kuijpers geleverde softwarepakket *Milestone Expert*. Milestone-meldkamers zijn beschikbaar op locatie Delft, Zoetermeer, Poseidon en de Hoofdlocatie. De Meldkamer op de Hoofdlocatie is de enige meldkamer waar alle camera's van alle locaties bekeken kunnen worden en waar beelden kunnen worden teruggekeken. De overige locaties kunnen alleen de beelden van de eigen locatie inzien en kunnen geen beelden terugkijken.

Aanvullend zijn de camerabeelden beschikbaar op de cliënt van het Security Management Systeem (SMS) in de meldkamer van de Hoofdlocatie. Op locatie Delft worden de camerabeelden ook live bekeken via een Security Management Systeem, deze meldkamer kan geen beelden terugkijken.

De Sportcampus kent een gedeeld eigenaarschap, waarbij de drie eigenaren zelf verantwoordelijk zijn voor specifieke delen van het pand, ook voor wat betreft cameratoezicht. Mocht het nodig zijn om camerabeelden gemaakt door het systeem van De Haagse Hogeschool te bekijken in het kader van interne opsporing (externe opsporing, zoals door politie, wordt beschreven in artikel 6.3) bij een van de twee andere eigenaren, dan nemen zij contact op met Team Veiligheid van De Haagse Hogeschool, via veiligheid@hhs.nl.

4. Taken, verantwoordelijkheden en bevoegdheden

4.1 Taken

a) Het CvB ziet toe op de correcte uitvoer van het vastgestelde cameraprotocol, welke is gedelegeerd aan de Directeur FZ&IT. Het CvB beslist over aanvragen met betrekking tot heimelijk te plaatsen camera's;
b) De Directeur FZ&IT draagt zorg voor een goede uitvoering en naleving van het protocol cameratoezicht, waaronder het uitvoeren van een DPIA. De Directeur FZ&IT beslist over beleid en aanvragen met betrekking tot camera's;
c) De Adviseur Veiligheid en de Functionaris Gegevensbescherming (FG) adviseren de Directeur FZ&IT aangaande beleidsmatig te nemen acties;
d) Waar het om specifieke plaatsing van camera's gaat, adviseert de Adviseur Veiligheid aan de Directeur FZ&IT over aanvragen vanuit de organisatie, aan de hand van dit protocol.
e) Waar het om specifieke heimelijke plaatsing van camera's gaat, adviseert de Adviseur Veiligheid in samenspraak met de FG aan de Directeur FZ&IT over aanvragen vanuit de organisatie, aan de hand van dit protocol. De Directeur FZ&IT legt deze aanvraag en het advies voor aan het CvB ter goedkeuring.
f) De beveiliging van De Haagse Hogeschool bekijkt de beelden van het camerasysteem gedurende openingstijden continu, en registreert terugkijken en bewaren van de beelden.
g) De afdeling Beheer en Onderhoud (B&O) draagt zorg voor aanleg, onderhoud en verwijdering van camerasystemen. Momenteel voert technisch dienstverlener Kuijpers (https://www.kuijpers.nl/) de opdrachten daadwerkelijk uit;
h) Kuijpers schakelt met de afdeling ICT en dragen zo samen zorg voor aansluiting van camera's op het systeem, het geautomatiseerd wissen van de beelden na het verstrijken van de bewaartermijn en dragen zorg voor de toepassing van passende technische maatregelen om verlies, misbruik of oneigenlijk gebruik van camerabeelden tegen te gaan.

4.2 Verantwoordelijkheden

a) Het CvB is verantwoordelijk voor de inhoud en vaststelling van het protocol in de zin van de AVG.
b) De Directeur FZ&IT is verantwoordelijk voor de naleving van het protocol cameratoezicht en het uitvoeren van een DPIA en juiste borging en (versie)beheer ervan in de privacy-administratie.
c) De beveiliging is verantwoordelijk voor het dagelijks cameratoezicht van de

betreffende locatie en veiligstellen van de beelden bij incidenten.

d) Bij overdracht van beelden aan het extern bevoegd gezag (bijv. Politie of Justitie) dient er een logboek bijgehouden te worden. De beveiliging houdt voornoemd logboek bij middels opname in de dagrapportage.
e) Eenieder voor wie niet reeds uit hoofde van ambt, beroep of wettelijk voorschrift een geheimhoudingsplicht geldt, is bij omgang met vertrouwelijke camerabeelden verplicht zich aan deze geheimhoudingsplicht te houden.
f) Iedereen die in aanraking komt met het camerasysteem draagt zorg voor een integere omgang met camerabeelden.

4.3 Beslissingskader Cameraplaatsing

Vóór de plaatsing van een camera, wordt de Adviseur Veiligheid om advies gevraagd. De Adviseur Veiligheid toetst de aanvraag aan de hand van:

- De uitgangspunten zoals genoemd in Hoofdstuk 3 van dit protocol;
- De mogelijkheid van alternatieve maatregelen;
- Financieel-economische afweging: welke schade wordt voorkomen tegen welke prijs? Nota bene: een doel als 'veiligheidsbeleving vergroten' is niet kostenmatig te kwantificeren. Voor dergelijke aanvragen neemt de Adviseur Veiligheid met het desbetreffende management contact op om gezamenlijk tot een afweging te komen.
- Privacy-afweging: de te voorkomen schade moet opwegen tegen de inbreuk op de privacy van geregistreerde personen. De variabelen voor deze afweging zijn of en welke materiele en/of immateriële schade voorkomen wordt, of cameratoezicht wel of niet verwacht kan worden op de locatie, welke andere beelden dan bedoeld gemaakt kunnen worden en de (on)wenselijkheid daarvan. De reeds uitgevoerde DPIA zal met deze afwegingen worden aangevuld.

Voornoemde punten komen allemaal terug in het advies dat de Adviseur Veiligheid bij de aanvraag voegt, ten behoeve van de beoordeling door de Directeur FZ&IT.

4.4 Technisch Beheer en Plaatsing

Het team Beheer en Onderhoud (B&O) heeft een Meerjaren Onderhoudsplan (MOP), waarbinnen het onderhoud en eventuele reparaties, het verhangen, verwijderen, controleren van camera's is opgenomen. Indien er iets met bestaande camera's gedaan moet worden dan valt dit onder dit MOP, wat via TopDesk aangevraagd kan worden.

Bij plaatsing van een *nieuwe* camera wordt de volgende procedure gehandhaafd.

1. De wens om een cameraplaatsing wordt voorgelegd aan de Adviseur Veiligheid die de aanvraag beoordeelt aan de hand van dit protocol, Hoofdstuk 4.3;
2. Bij Beheer en Onderhoud (B&O) wordt een uitvraag gedaan voor kosten en

systeemwensen;

3. Nadat vooronderzoek wenselijkheid, kosten enzovoort is afgerond zal het voorstel, met advies, ter goedkeuring worden voorgelegd aan de Directeur FZ&IT;
4. Nadat is vastgesteld welk type camera er geplaatst moet worden zal B&O de opdracht doorzetten naar de installateur;
5. Na plaatsing van de camera zal deze beschikbaar gesteld worden in Milestone en het Security Management Systeem in de meldkamer van de Hoofdlocatie door Kuijpers samen met de betreffende IT-afdeling.

Valt een aanvraag niet binnen voornoemd protocol, dan geven de Adviseur Veiligheid en de FG een negatief advies aan de Directeur FZ&IT. Wanneer het een situatie betreft die niet is beschreven in het bestaande protocol, zal een nieuwe toetsing plaatsvinden zoals beschreven in paragraaf 4.3. Bij verbouwingen of werkzaamheden waarbij het gebied een nieuwe indeling of functie zal krijgen zal de Adviseur Veiligheid bepalen of de aanwezige camera's nog steeds gewenst zijn.

4.5 Bevoegdheden met betrekking tot het bekijken van de camerabeelden

De volgende functionarissen zijn bevoegd, binnen het kader van de doelstelling zoals omschreven in artikel 1, camerabeelden te bekijken en terug te kijken, onder voorwaarde dat dit alleen beelden betreft waar de genoemde functionaris verantwoordelijkheid over draagt:

- Directeur FZ&IT
- Hoofd Beveiliging
- Adviseur Veiligheid
- Beveiligers zolang het de opnames tijdens de eigen dienst betreft, of in opdracht van bovenstaande functionarissen.

De volgende functionarissen zijn bevoegd, binnen het kader van de doelstelling zoals omschreven in artikel 1, live camerabeelden te bekijken:

- Beveiligers
- Receptionisten van de Frontoffice
- Medewerkers Toezicht en support

Onder verantwoordelijkheid en na toestemming van de Directeur FZ&IT kunnen overige personen toestemming verkrijgen om incidenteel camerabeelden te bekijken, onder voorwaarde dat de betreffende persoon een zwaarwegend, gerechtvaardigd belang heeft en de privacy van de betrokkene niet onrechtmatig wordt geschaad. De Adviseur Veiligheid, de beveiliging en aangewezen personen van B&O en ICT, die te maken hebben met de camera's, krijgen een AVG-instructie van de FG, om te borgen dat conform regelgeving met camerabeelden wordt omgegaan. Voordat een overig persoon beelden kan bekijken, selecteert het Hoofd Beveiliging de relevante beelden en zorgt ervoor dat enkel die bekeken kunnen worden.

5. Camerabeelden

5.1 Bewaartermijn

Gezien de geldende wettelijke eisen, is het van belang een duidelijke bewaartermijn van camerabeelden te definiëren. De bewaartermijn is volgens de richtlijn van de Autoriteit Persoonsgegevens maximaal 28 dagen. De Haagse Hogeschool hanteert dan ook een bewaartermijn van 28 dagen. Deze termijn is gebaseerd op de doelstellingen waarvoor cameratoezicht wordt ingezet zoals genoemd in Hoofdstuk 2 van dit protocol. Daarnaast geeft de omgeving van het onderwijs voldoende reden voor deze bewaartermijn in verband met schoolvakanties, waarbij soms langere tijd niemand aanwezig is op de betreffende locatie. Bij vermoeden van strafbare feiten moeten beelden nog te raadplegen zijn. Uitzonderingen op de reguliere bewaartermijn kunnen dus worden gemaakt na incidenten.
Bij het verlopen van de bewaartermijn worden de camerabeelden automatisch gewist, Milestone Expert is zodanig geprogrammeerd. Camera's kunnen bepaalde incidenten vastleggen of de beelden kunnen dienen als bewijsmateriaal in een strafprocedure. Deze beelden dienen bewaard te worden totdat het geconstateerde incident is afgehandeld of bij overdracht aan extern bevoegd gezag.

5.2 Heimelijk toezicht

Heimelijk toezicht betreft het toezicht met behulp van verborgen en/of niet zichtbare camera's of cameratoezicht dat niet kenbaar is gemaakt aan studenten, medewerkers en bezoekers. Heimelijk toezicht is verboden, tenzij dit noodzakelijk is voor zeer zorgelijke situaties. Ook het heimelijk maken van geluidsopnames, al dan niet met daartoe geschikte camera's, zoals beschreven in het Wetboek van Strafrecht Artikel 139a en b, is verboden.
Heimelijk toezicht dient altijd een tijdelijk karakter te hebben en is met grote waarborgen omkleed ter bescherming van de privacy. Het inzetten van heimelijk cameratoezicht is niet mogelijk voor preventieve doeleinden. Inzet van heimelijk toezicht is alleen toegestaan na akkoord van het CvB. De Directeur FZ&IT legt, op basis van advisering door de Adviseur Veiligheid en de FG, hiervoor een voorstel ter besluitvorming voor. Heimelijk toezicht is bedoeld als laatste redmiddel en wordt zeer beperkt ingezet. Voordat heimelijk cameratoezicht mag worden ingezet wordt een nieuwe DPIA uitgevoerd. Als daar een hoog privacyrisico uit blijkt meldt het CvB, in samenspraak met de FG, haar voornemen bij de Autoriteit Persoonsgegevens. Er wordt in dat geval pas aangevangen met heimelijk cameratoezicht na instemming van de Autoriteit Persoonsgegevens.

5.3 Terugkijken van beelden door derden

Het is verboden om camerabeelden zonder aanleiding terug te kijken. Voor terugkijken van camerabeelden dient er sprake te zijn van een vermoeden van een strafbaar feit, waarbij de beelden kunnen dienen als bewijsmateriaal. Terugkijken van beeldmateriaal is alleen toegestaan als een zwaarwegend belang kan worden aangetoond en loopt via de Adviseur Veiligheid, zie ook paragraaf 4.5.

Een geregistreerde medewerker of student heeft het recht van inzage slechts wanneer op grond van opgenomen beelden door hem verantwoording over zijn handelen moet worden afgelegd.

De beslissing over de aanvraag geschiedt binnen *2 werkdagen*. Zolang er geen besluit is genomen worden de betreffende beelden bewaard.

Medewerkers of studenten kunnen gevraagd worden beelden te bekijken, alleen ter identificatie van betrokkenen bij incidenten.

5.4 Afgifte informatie aan extern bevoegd gezag

Op vordering van het extern bevoegd gezag (Politie of Officier van Justitie) moet beeldinformatie verstrekt worden, wanneer hiernaar gevraagd wordt onder verwijzing naar de wettelijke regeling die hieraan ten grondslag ligt, dan wel indien dit noodzakelijk is voor de publiekrechtelijke taakuitvoering. Hierbij is het volgende stappenplan van toepassing:

1. De functionaris die de beelden wil ontvangen legitimeert zich ten overstaan van het Hoofd Beveiliging en omschrijft het tijdvak en de inhoud van de gevraagde beelden.
2. Daarna worden de beelden in principe door middel van DVD en/of USB meegegeven, waarbij de beelden gemerkt zijn door Milestone Expert. Alleen middels deze software zijn de beeldwerken zichtbaar.
3. De ontvangende functionaris tekent voor ontvangst en zorgvuldig gebruik van de beeldinformatie (zie ‘formulier afgifte beelden’, bijlage 2).
4. Het getekende exemplaar van het ‘formulier afgifte beelden’ wordt bewaard door het Hoofd Beveiliging en gerapporteerd in het kwartaaloverzicht, een kopie is voor de ondertekenaar en minimaal eens per jaar gaat een (verzamel)melding naar de Directeur FZ&IT, met in cc de Adviseur Veiligheid.

6. Verantwoording, Herziening en goedkeuring

6.1 Verantwoording

De volgende functionarissen leggen verantwoording af:

- De medewerkers van de beveiliging leggen verantwoording af aan het Hoofd Beveiliging.
- Het Hoofd Beveiliging legt verantwoording af aan de Adviseur Veiligheid
- De Adviseur Veiligheid legt verantwoording af aan de Directeur FZ&IT
- De Directeur FZ&IT legt verantwoording af over de uitvoer van dit protocol aan het CvB middels een jaarverslag.
- De Directeur FZ&IT zal tenminste eens per drie jaar het protocol cameratoezicht (laten) herzien. Hierna zal het protocol ter vaststelling worden voorgelegd aan het CvB.

6.2 Instemming Hogeschoolraad

Art. 7 lid 7 sub b van het Medezeggenschapsreglement Haagse Hogeschool 2017 vermeldt “Het College van Bestuur behoeft de instemming van de hogeschoolraad voor het door hem voorgenomen besluit met betrekking tot: vaststelling of wijziging van de regels ter voorkoming en bestrijding van ongewenst gedrag en de bescherming van de privacy (reglement ongewenst gedrag, privacyreglement).”

Dit protocol cameratoezicht dient op grond van dit artikel te worden voorgelegd aan de Hogeschoolraad. De Hogeschoolraad heeft instemmingsrecht op het cameraprotocol.

7. Klachten

Klachten over de uitvoering en toepassing van het cameratoezicht kunnen schriftelijk worden ingediend bij het Hoofd Beveiliging, of kunnen worden gemeld bij de Frontoffice. Wanneer de Hoofd Beveiliging aanleiding ziet voor nader onderzoek, dient de Directeur FZ&IT geïnformeerd te worden via de Adviseur Veiligheid. Er wordt gezocht naar een passende oplossing. Indien de klager niet tevreden is met de afhandeling van de klacht kan deze binnen zes weken na de dag van constatering een beroep doen op de klachten- en bezwarenprocedures van De Haagse Hogeschool:

https://dehaagsehogeschool.sharepoint.com/sites/ServicePlein/SitePages/ik-heb-een-klacht.aspx.

8. Slotbepalingen

Bij afwezigheid van de genoemde functionaris in het protocol cameratoezicht, is diens plaatsvervanger verantwoordelijk.
In alle gevallen, waarin dit protocol cameratoezicht niet voorziet, beslist de Directeur FZ&IT, geadviseerd door de Adviseur Veiligheid.

Bijlage 1

Begrippenlijst

Begrip	**Toelichting**
Autoriteit Persoonsgegevens (AP)	De AP houdt toezicht op de naleving van de wettelijke regels voor bescherming van persoonsgegevens
AVG	De Algemene Verordening Gegevensbescherming. Dit is een Europese verordening die de regels voor de verwerking van persoonsgegevens door particuliere bedrijven en overheidsinstanties in de Europese Unie standaardiseert en de bescherming van persoonsgegevens garandeert.
Cameratoezicht	Toezicht met behulp van camera's, waardoor er sprake is van verwerking van persoonsgegevens als bedoeld in de Algemene Verordening Gegevensbescherming. Hierbij wordt er gesproken over het gehele camerasysteem (camera's, uitkijken van beelden en het opslaan van beelden).
Camerasysteem	Het geheel van camera's, monitoren, opname, afspeel- en printapparatuur waarmee toezicht kan worden uitgeoefend.
Campus	Verzamelterm voor gebouw of verzameling gebouwen
Meldkamer	Ruimte waar camerabeelden verzameld en bekeken worden
College van Bestuur	Het bevoegd gezag van De Haagse Hogeschool
Extern bevoegd gezag	Een partij van buiten De Haagse Hogeschool, zoals de politie of de Officier van Justitie, die ter uitvoering van een wettelijke, publiekrechtelijke taak of bevoegdheid gerechtigd is om instructies te geven aan De Haagse Hogeschool met betrekking tot onderwerpen die in dit Protocol zijn vastgelegd, zoals het opvragen en beschikbaar houden van camerabeelden
Functionaris Gegevensbescherming	Ingevolge de Algemene Verordening Gegevensbescherming aangewezen medewerker van De Haagse Hogeschool belast met het toezicht op de verwerking van persoonsgegevens bij De Haagse Hogeschool.
Heimelijk toezicht	Al het toezicht met behulp van verborgen en/of niet zichtbare camera's of cameratoezicht dat niet kenbaar is gemaakt aan studenten, medewerkers en bezoekers
Incident	Een waargenomen ongewenst en/of strafbaar feit, ongeval of andere gebeurtenis die vraagt om handhaving, onderzoek en/of strafrechtelijke vervolging.
Protocol Cameratoezicht	Inhoudelijke verantwoording en handelingswijze inzake de omgang met het camerasysteem en camerabeelden

Bijlage 2

Formulier afgifte camerabeelden

Hierbij verklaart ondergetekende camerabeelden te ontvangen van
De Haagse Hogeschool [Locatie]

Voor- en achternaam:
……

Functie:
……

Organisatie:
……

Identificatiebewijs en –nummer
……

Incident:
……

Tijdspanne:
……

Datum van incident:
……

Camerapositie(s):
……

Op grond van het proces verbaal d.d.:/
Het besluit van de Directeur FZ&IT d.d.:
……

Handtekening ontvanger:
……

Plaats:
……

Datum:
……

Handtekening Hoofd Beveiliging:
……

- Origineel formulier blijft in bezit betreffend hoofd Beveiliging
- Kopie formulier per mail naar Directeur FZ&IT en Adviseur Veiligheid
- Kopie formulier voor ontvanger

Bijlage 3

Logboek afgifte camerabeelden

De Haagse Hogeschool [Locatie]

Nr.:	Datum afgifte:	Incident:	Afgifte aan:
1.	.....	.....	.....
2.	.....	.....	.....
3.	.....	.....	.....
4.	.....	.....	.....
5.	.....	.....	.....
6.	.....	.....	.....
7.	.....	.....	.....
8.	.....	.....	.....
9.	.....	.....	.....
10.	.....	.....	.....
11.	.....	.....	.....
12.	.....	.....	.....
13.	.....	.....	.....
14.	.....	.....	.....
15.	.....	.....	.....
16.	.....	.....	.....
17.	.....	.....	.....
18.	.....	.....	.....
19.	.....	.....	.....
20.	.....	.....	.....