

Videocameratoezicht

Reglement



Colofon

Op de campus en binnen de gebouwen van [Organisatie] vindt videocameratoezicht plaats voor de beveiliging van goederen, gebouwen en personen. Het cameratoezicht maakt deel uit van een totaalpakket aan maatregelen rondom integrale veiligheid binnen de organisatie. Dit reglement vormt het kader waarbinnen het cameratoezicht binnen [Organisatie] plaatsvindt.

Bestemd voor

Dit document is bestemd voor medewerkers, studenten en bezoekers van [Organisatie].

Samenstelling en beheer

Dit document is tot stand gekomen via het Privacy Expertise Centrum van SURF. Het beheer van dit document berust bij SURF.

Licentie

Dit document is verstrekt onder de creative commons-licentie [CC BY](#) 4.0 International (naamsvermelding). SURF aanvaardt geen aansprakelijkheid voor enig gebruik/toepassing van dit document.

Versiebeheer

Versie	Door	Datum	Toelichting/wijziging
1.0			Initieel document

Inhoudsopgave

Colofon	2
1 Inleiding	4
2 Doelstelling en randvoorwaarden	4
2.1 Doelstelling	4
2.2 Verantwoordelijkheid	4
2.3 Wetgeving	4
2.4 Informatieplicht/transparantie	5
2.5 Bewaartermijn camerabeelden	5
2.6 Autorisatie	5
2.7 Inzageverzoeken	5
3 Reglement Videocameratoezicht (CCTV)	5
Artikel 1 – Begripsbepalingen	5
Artikel 2 – Werkingssfeer en doelstellingen cameratoezicht	7
Artikel 3 – Taken en verantwoordelijkheden	7
Artikel 4 – Inrichten camerasysteem en beveiliging	8
Artikel 5 – Inzage en uitgifte opgenomen camerabeelden aan derden	9
Artikel 6 – Rechten van betrokkenen	9
Artikel 7 – Heimelijk cameratoezicht	9
Artikel 9 – Verslaglegging en rapportage	10
Artikel 10 – Slotbepalingen	10
4 Controle en evaluatie	10

1 Inleiding

Cameratoezicht kan een inbreuk op de privacy van medewerkers, studenten en bezoekers met zich meebrengen. De AVG stelt daarom eisen aan het gebruik van cameratoezicht, waarbij het uitgangspunt is dat de inbreuk zo klein mogelijk blijft. Mensen moeten onbevangen zichzelf kunnen zijn.

Dit reglement vormt het kader waarbinnen het cameratoezicht binnen [Organisatie] plaatsvindt. Het geeft een beschrijving van taken, verantwoordelijkheden en procedures over het cameratoezicht, met het oog op integer gebruik van het camerasysteem en de bescherming van privacy van aanwezigen op de campus.

Dit beleid vloeit voort uit het security- en privacybeleid en -reglementen voor medewerkers en studenten, waarin onder andere is geregeld hoe [Organisatie] omgaat met persoonsgericht onderzoek.

2 Doelstelling en randvoorwaarden

2.1 Doelstelling

- Het voorzien in een onderdeel van een pakket fysieke beveiligingsmaatregelen op de campus voor de veiligheid van de aanwezigen.
- Het respecteren van de privacy van de betrokkenen door te zorgen voor adequate gegevensbescherming.
- Het voldoen aan geldende wet- en regelgeving.

2.2 Verantwoordelijkheid

De eindverantwoordelijkheid voor het inzetten van videocameratoezicht ligt bij het College van Bestuur (CvB). Het CvB kan een deel van haar beslissingsbevoegdheid overdragen aan één of meerdere personen in de organisatie om praktisch uitvoering te geven aan het cameratoezicht (zoals de CIO of hoofd beveiliging).

De OR en de SR hebben instemmingsrecht over dit reglement met de randvoorwaarden en waarborgen waaraan het videocameratoezicht moet voldoen.

2.3 Wetgeving

De wetgever geeft een onderwijsinstelling een aantal randvoorwaarden mee waar cameratoezicht aan moet voldoen, waaronder de Algemene verordening gegevensbescherming (AVG). De toezichthouder Autoriteit Persoonsgegevens geeft hierover informatie specifiek gericht op scholen¹.

[Organisatie] heeft een gerechtvaardigd belang om videocameratoezicht in te zetten. Deze verwerkingsgrondslag zoals bedoeld in de AVG is uitgewerkt in de DPIA die door [Organisatie] is gemaakt voor het inzetten van videocameratoezicht.

¹ AP: [cameratoezicht op scholen](#)

2.4 Informatieplicht/transparantie

[Organisatie] zorgt ervoor dat studenten, medewerkers en bezoekers kunnen weten dat er camera's hangen. Dit is aangegeven met bordjes en stickers bij de ingangen. Het reglement is op het intranet gepubliceerd, toegankelijk voor zowel medewerkers als studenten.

2.5 Bewaartermijn camerabeelden

De richtlijn van de Autoriteit Persoonsgegevens voor het bewaren van camerabeelden is gesteld op maximaal 4 weken. Daarna moeten de beelden worden vernietigd. [Organisatie] bewaart de camerabeelden niet langer dan noodzakelijk. De opnames worden maximaal zeven dagen bewaard. Vervolgens worden ze automatisch gewist/overschreven, tenzij er sprake is van een incident (diefstal, fraude of mishandeling, etc.). Opnames van incidenten worden verwijderd zodra het incident is afgehandeld.

2.6 Autorisatie

De toegang tot en het gebruik van de camera's en opgenomen camerabeelden is adequaat beveiligd. Binnen [Organisatie] zijn afspraken gemaakt over wie en onder welke voorwaarden personen toegang hebben tot de beelden en eventueel het terugkijken ervan.

2.7 Inzageverzoeken

De wet geeft personen het recht om beelden te bekijken waarop zijzelf te zien zijn. Het gaat daarbij nadrukkelijk om beelden van de persoon in kwestie en niet om beelden enkel van eigendommen of beelden waarop ook andere personen te zien zijn. Dit recht is niet absoluut. Een inzageverzoek mag worden afgewezen wanneer het inzageverzoek niet is gespecificeerd of als het inzagerecht kennelijk wordt misbruikt. Daarnaast mag een inzageverzoek worden geweigerd als dat noodzakelijk is in het belang van het voorkomen, opsporen en vervolgen van strafbare feiten.

Derden krijgen uitsluitend toegang tot camerabeelden als de betrokkene daarvoor uitdrukkelijke toestemming geeft of wanneer de verstrekking noodzakelijk is op grond van een wettelijke verplichting of voor de goede vervulling van de (publiekrechtelijke) taak van politie en justitie in het geval van incidenten en opsporing. Zie de privacyreglementen van [Organisatie] voor meer informatie.

3 Reglement Videocameratoezicht (CCTV)

Artikel 1 – Begripsbepalingen

In dit reglement wordt verstaan onder:

Beheerder	de door de Verantwoordelijke aangewezen medewerker van [Organisatie] die verantwoordelijk is voor de inrichting, het beheer en toezicht op het cameratoezicht
Bevoegde medewerker	een door de (locatie)beheerder als zodanig aangewezen persoon die betrokken is bij de uitvoering van het cameratoezicht

Verwerker	het bedrijf of organisatie die door [Organisatie] wordt ingehuurd om een deel van het cameratoezicht te verzorgen
Bezoeker	een natuurlijke persoon, niet zijnde een student of een medewerker
Camerabeeld	het door het cameratoezicht verkregen camerabeeld
Camera-observatieruimte	een centraal gesitueerde, van een toegangscontrolesysteem voorziene ruimte, waarin de camerabeelden - van alle locaties - centraal live worden bekeken en/of waar ook de mogelijkheid bestaat om opgenomen camerabeelden terug te kijken en/of op een informatiedrager te plaatsen
Cameratoezicht	toezicht met behulp van camera's, waardoor er sprake is van verwerking van persoonsgegevens als bedoeld in de Algemene verordening gegevensbescherming (AVG)
Camerasysteem	het geheel van camera's, monitoren, opnameapparatuur, verbindingkasten en verbindingen waarmee het cameratoezicht wordt uitgevoerd
[Organisatie]	Stichting[Organisatie], gevestigd te [plaats], dan wel haar College van Bestuur of gevolmachtigde(n)
Heimelijk cameratoezicht	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
Locatiebeheerder	een door de beheerder als zodanig aangewezen persoon die belast is met het cameratoezicht op één of meerdere locaties van [Organisatie] (hoofd Integrale Veiligheid, Beveiliging & Services)
Medewerker	degene die voor en/of namens [Organisatie] werkzaamheden verricht (via een arbeids- en/of uitzendovereenkomst, detachering of anderszins).

Serverruimte	de van een toegangscontrolesysteem voorziene ruimte, waar de server of opnameapparatuur staat waarop de opgenomen camerabeelden geregistreerd staan
Student	degene die met [Organisatie] een onderwijsovereenkomst is aangegaan in de beroepsopleidende leerweg (BOL) dan wel beroepsbegeleidende leerweg (BBL) in de zin van de Wet educatie en beroepsonderwijs dan wel als extraneus is ingeschreven en betrokkene is
Technisch beheerder	de functionaris, die onder verantwoordelijkheid van de beheerder, is belast met het technisch beheer van het camerasysteem (Beveiligers)
Verantwoordelijke	het College van Bestuur van [Organisatie] of gevolmachtigde(n)

Artikel 2 – Werkingssfeer en doelstellingen cameratoezicht

1. Dit reglement is van toepassing op al het cameratoezicht binnen [Organisatie].
2. Het inzetten van cameratoezicht, en het gebruik van de camerabeelden, is alleen toegestaan voor:
 - a. de bescherming van de veiligheid en gezondheid van studenten, medewerkers en bezoekers;
 - b. de beveiliging van de toegang tot gebouwen en terreinen, waaronder mede is begrepen het weren van onbevoegde of onbevoegd verklaarde personen;
 - c. de bewaking van zaken die zich in gebouwen of op terreinen bevinden;
 - d. het vastleggen van incidenten.
3. Camerabeelden worden uitsluitend gebruikt voor de doelstelling zoals genoemd in lid 2. [Organisatie] gebruikt het videocameratoezicht niet voor het beoordelen van het functioneren van medewerkers of studenten.
4. In ruimtes waar men ongestoord moet kunnen zijn, zoals toiletten, douches en kleed- en kolfruimten, is het niet toegestaan een camera te plaatsen.

Artikel 3 – Taken en verantwoordelijkheden

1. Het cameratoezicht vindt plaats onder verantwoordelijkheid van de Verantwoordelijke.
2. Voordat wordt besloten tot het instellen of intensiveren van cameratoezicht, voert de Verantwoordelijke een privacytoets uit (DPIA), waarbij de mate van inbreuk op de privacy van de studenten, medewerkers en bezoekers wordt afgewogen tegen het belang van [Organisatie] om cameratoezicht te gebruiken. Hierbij wordt meegewogen of de doelstellingen als geformuleerd in artikel 2 tweede lid, op een andere wijze kunnen worden bereikt, met een minder ingrijpend middel dan cameratoezicht.
3. De Verantwoordelijke wijst een beheerder aan die verantwoordelijk is voor de inrichting, het beheer en toezicht op het cameratoezicht binnen [Organisatie], alsmede een technisch beheerder die, onder verantwoordelijkheid van de beheerder, belast is met het technisch beheer van het camerasysteem.
4. De beheerder wijst bevoegde medewerkers aan, en zo nodig een of meer locatiebeheerder(s).

5. De beheerder wijst voor zichzelf en voor de locatiebeheerder een plaatsvervanger aan, die in geval van afwezigheid van de beheerder respectievelijk locatiebeheerder in diens taken en verantwoordelijkheden treedt.
6. De beheerder, locatiebeheerder(s) en bevoegde medewerkers zijn bevoegd tot het live uitkijken van camerabeelden.
7. De beheerder en locatiebeheerder zijn bevoegd tot het terugkijken en uitgeven (zoals bedoeld in artikel 5) van opgenomen camerabeelden. In gevallen waar het nodig is om terug te kijken om te zien wat ergens gebeurt, kan dit plaatsvinden door een bevoegde medewerker met de locatiebeheerder. Als het gaat om beelden terug te kijken om te zien om wie een bepaalde situatie gaat, gebeurt dit uitsluitend door de beheerder en locatiebeheerder.
8. De beheerder en locatiebeheerder kunnen een bevoegde medewerker autoriseren om – onder verantwoordelijkheid van de beheerder of locatiebeheerder – onder nader te stellen voorwaarden en voor een vooraf bepaald doel c.q. een vooraf bepaalde periode camerabeelden terug te kijken.
9. Als het terugkijken van beelden gebeurt in relatie tot inhoudelijk persoonsgericht onderzoek, worden de voorwaarden zoals vermeld in het ICT-reglement gevolgd. In die gevallen is er is een opdracht nodig van de Verantwoordelijke en er vindt afstemming plaats met de privacyfunctionaris.
10. In geval de Verantwoordelijke een verwerker inschakelt, geeft deze de verwerker de opdracht om te handelen volgens dit reglement.

Artikel 4 – Inrichten camerasysteem en beveiliging

1. De Verantwoordelijke is verantwoordelijk voor de inrichting van het camerasysteem en de plaatsing van de camera's, binnen de kaders van de door de Verantwoordelijke uitgevoerde privacytoets als bedoeld in artikel 3 lid 2.
2. De Verantwoordelijke zorgt voor passende technische en organisatorische maatregelen om de camerabeelden te beveiligen tegen verlies of tegen enige vorm van onrechtmatig gebruik. Deze maatregelen garanderen, rekening houdend met de stand van de techniek (zoals te doen gebruikelijk in de informatiebeveiligings- en beveiligingsbranche) en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's van het cameratoezicht en de aard van te beschermen camerabeelden met zich meebrengen. De maatregelen betreffen het camerasysteem, de serverruimte en camera-observatieruimte.
3. De met cameratoezicht belaste medewerkers gaan vertrouwelijk en integer om met de kennis die zij tot zich nemen vanwege het cameratoezicht, in het bijzonder met betrekking tot de privacy van studenten, medewerkers en bezoekers. Voor zover daar arbeidsrechtelijk niet in is voorzien, sluit de beheerder daartoe een geheimhoudingsverklaring met de locatiebeheerder(s), technisch beheerder en/of bevoegde medewerker(s).
4. De beheerder zorgt ervoor dat het cameratoezicht kenbaar wordt gemaakt aan studenten, medewerkers en bezoekers op zichtbare en herkenbare wijze, zoals, maar niet beperkt tot, borden en stickers bij de ingang van de gebouwen of terreinen van [Organisatie].
5. Voor zover er in het camerasysteem camerabeelden worden opgeslagen, worden deze beelden uiterlijk vier weken na de opname automatisch gewist, tenzij er een incident is geconstateerd op basis waarvan het noodzakelijk is de met het incident samenhangende camerabeelden te bewaren. Na afhandeling van het incident worden de betreffende camerabeelden (en eventueel gemaakte kopieën of afdrukken) gewist.
6. Het camerasysteem is zodanig uitgerust dat het terugkijken van opgenomen camerabeelden of het uitgeven daarvan slechts mogelijk is in de camera-observatieruimte.

7. Voor zover er live camerabeelden worden uitgekeken in een andere ruimte dan de serverruimte of camera-observatieruimte, zijn er technische en organisatorische maatregelen genomen die het onbevoegd meekijken zoveel als redelijkerwijs mogelijk voorkomen.
8. Voor zover er bij het inrichten van het camerasysteem voor gekozen wordt om de studenten, medewerkers en bezoekers via een monitor live terugkoppeling te geven van de camerabeelden, kunnen deze live camerabeelden alleen betrekking hebben op deze betreffende studenten, medewerkers en bezoekers.
9. Het bewerken van camerabeelden gebeurt alleen met het doel de camerabeelden te verscherpen.

Artikel 5 – Inzage en uitgifte opgenomen camerabeelden aan derden

1. Op verzoek van politie, rechter-commissaris of (hulp)officier van justitie kan inzage worden gegeven in (opgenomen) camerabeelden in het kader van de uitoefening van diens publiekrechtelijke taak.
2. Uitgifte van camerabeelden vindt slechts plaats op vordering van de politie, rechter-commissaris of (hulp)officier van justitie mits de vordering gebaseerd is op een wettelijke grondslag.
3. Alvorens tot inzage of uitgifte over te gaan, legitimeert de betreffende functionaris zich vooraf ten overstaan van de beheerder of locatiebeheerder, en tekent voor ontvangst van de uitgegeven camerabeelden.
4. De inzage en uitgifte wordt door de beheerder of locatiebeheerder geregistreerd.
5. Aan andere derden wordt geen inzage in de camerabeelden gegeven, of camerabeelden uitgegeven, anders dan met de uitdrukkelijke schriftelijke toestemming van de betrokken student, medewerker of bezoeker.

Artikel 6 – Rechten van betrokkenen

1. Betrokken studenten, medewerkers en bezoekers mogen specifieke rechten uitoefenen zoals bedoeld in de Algemene Verordening Gegevensbescherming. Hieronder vallen het recht op inzage in en correctie en verwijdering van camerabeelden waarop zij herkenbaar zijn.
2. Een verzoek tot inzage in en correctie en verwijdering van camerabeelden wordt afgehandeld door de Privacy Officer volgens de daarvoor afgesproken procedure. Zie ook hoofdstuk 1 'Randvoorwaarden'.

Artikel 7 – Heimelijk cameratoezicht

1. Heimelijk cameratoezicht is alleen toegestaan als er sprake is van (een redelijk vermoeden van) diefstal, fraude en/of vernieling en/of andere incidenten en regulier cameratoezicht en andere door [Organisatie] genomen maatregelen en inspanningen, niet hebben geleid tot beëindiging van deze incidenten. Het inzetten van heimelijk cameratoezicht is niet mogelijk voor preventieve doeleinden.
2. Heimelijk cameratoezicht mag alleen tijdelijk en op zodanige wijze worden ingezet, dat sprake is van een minimale inbreuk op de persoonlijke levenssfeer van de studenten, medewerkers en bezoekers.

3. Heimelijk cameratoezicht is uitsluitend toegestaan na specifieke voorafgaande schriftelijke toestemming van de Verantwoordelijke en onder vermelding van de voorwaarden waaronder het heimelijk cameratoezicht plaatsvindt.
4. [Organisatie] informeert voor zover redelijkerwijs mogelijk achteraf de betrokken personen over het toegepaste heimelijk cameratoezicht.
5. Voordat heimelijk cameratoezicht wordt toegepast, voert [Organisatie] een DPIA uit.

Artikel 9 – Verslaglegging en rapportage

De beheerder rapporteert ten minste jaarlijks schriftelijk aan de Verantwoordelijke over het toegepaste cameratoezicht, waaronder begrepen is een verslag over de verstrekkingen van camerabeelden zoals bedoeld in artikel 5.

Artikel 10 – Slotbepalingen

1. Dit reglement is, na instemming van de Ondernemingsraad en Studentenraad, vastgesteld door de Verantwoordelijke en per [variabele] in werking getreden.
2. Alle voorgaande reglementen en notities betreffende dit onderwerp komen te vervallen op het tijdstip van inwerkingtreding van dit reglement.
3. Dit reglement wordt aangehaald als: Reglement Videocameratoezicht CCTV [Organisatie].

4 Controle en evaluatie

Jaarlijks controleren de IBP-functionarissen van [Organisatie] steekproefsgewijs of de afgesproken regels worden nageleefd. Dit gebeurt in overleg met het hoofd Integrale Veiligheid.

Dit beleid wordt tweejaarlijks gecontroleerd en bijgesteld als dat nodig is. Hierbij zijn betrokken de IBP-functionarissen, [variabele], hoofd Integrale Veiligheid en de CIO.