PROTOCOL CAMERATOEZICHT

HOGESCHOOL
UTRECHT

Postbus 573
3500 AN
Utrecht

Tel 030 230 81 08
Fax 030 230 83 99
www.hu.nl

INLEIDING
Dit protocol ziet toe op het cameratoezicht binnen de Hogeschool Utrecht. Deze beeldinformatie wordt middels elektronische apparatuur vastgelegd. Het cameratoezicht is een verwerking in de zin van de Wet bescherming persoonsgegevens (Wbp).
Dit protocol geeft een beschrijving van taken, verantwoordelijkheden en procedures met het oog op een integer gebruik van het camerasysteem en de bescherming van de privacy.

Artikel 1. Doel van het cameratoezicht
Het doel van het cameratoezicht is om de veiligheid van personen, goederen en gebouwen in gebruik bij de Hogeschool Utrecht te bewaken. Deze vorm van toezicht is onderdeel van een breder pakket veiligheidsmaatregelen.
Meer specifiek is de verwachting dat het cameratoezicht bijdraagt aan:
• het bevorderen van het veiligheidsgevoel van personen die er werken of studeren;
• het bevorderen van de opsporing en vervolging van strafbare feiten;
• het voorkomen van diefstal en vandalisme.

Artikel 2. Begripsbepaling
1. camerasysteem: het geheel van camera's, monitoren, opnameapparatuur, verbindingskasten, verbindingen en bevestigingen;
2. videoruimte: de ruimte waarin de beelden opgenomen en teruggekeken kunnen worden;
3. beeldinformatie: de door het camerasysteem verkregen en geregistreerde filmbeelden;
4. beheerder: de leidinggevende die is belast met het beheren van het camerasysteem en de continuïteit van het cameratoezicht;
5. technisch beheerder: de medewerker die is belast met het onderhoud van het camerasysteem;
6. receptionist: de door de beheerder aangewezen persoon die de beelden live bekijkt;
7. geautoriseerde medewerker: de (beveiligings-)medewerker die bevoegd toegang heeft tot c.q. werkt in de videoruimte of derden die zich vooraf gelegitimeerd hebben en toestemming hebben van de geautoriseerde medewerker (onderhoud);
8. incident: een waargenomen strafbaar feit, ongeval of andere gebeurtenis die vraagt om optreden.

Artikel 3. Taken en verantwoordelijkheden
1. Het cameratoezicht geschiedt onder verantwoordelijkheid van het College van Bestuur (CvB), de houder van het camerasysteem.
2. De beheerder van het camerasysteem is de Manager van de Facilitaire Dienst.
3. Het technisch beheer van het cameratoezicht geschiedt door een door de beheerder aan te wijzen persoon/personen.
4. De beelden worden live bekeken door de receptionist die elke bijzonderheid meteen aan de beheerder rapporteert.

5. De kwaliteit van de beelden worden op gezette tijden gecontroleerd door de technische beheerder. Hij draagt zorg voor een optimale kwaliteit.
6. Ingeval van een incident meldt de beheerder dit bij de geëigende instantie (politie, brandweer, spoedeisende medische hulpverlening (ambulance) of gemeentelijke afdeling.

Artikel 4. De videoruimte
1. De ruimte waar de beelden worden opgeslagen is beveiligd tegen inbraak en vandalisme.
2. De ruimte is uitsluitend toegankelijk met de toestemming van de beheerder of diens vervanger.

Artikel 5. Bediening van het camerasysteem
1. Bevoegd tot het bedienen van het camerasysteem c.q. het live bekijken van beelden zijn:
   a. de receptionisten (alleen bekijken van live beelden);
   b. de technische beheerder (controle op de kwaliteit van de beelden);
   c. de beheerder of diens vervanger (volledig bevoegd);
   d. derden, indien dat functioneel noodzakelijk is, uitsluitend met toestemming van de beheerder of diens vervanger.
2. Onder volledig bevoegd wordt ook begrepen het terugkijken van digitale opnamen en het vastleggen van beeldinformatie op CD-ROM of een andere wijze van datatransport.

Artikel 6. Verslaglegging en rapportage
1. a. De beheerder houdt een logboek bij van het volledig bevoegd gebruik van het camerasysteem.
   b. De technisch beheerder houdt van de controle op juiste werking van het camerasysteem een logboek bij.
2. De logboeken zijn vertrouwelijk en uitsluitend ter inzage voor facilitair manager en CvB.
3. In de logboeken wordt vermeld: naam van de dienstdoende (technisch) beheerder, datum, tijd en bijzonderheden, zoals: storingen, incidenten, meldingen, vordering van beeldinformatie etc.
4. Buiten gebruik worden de logboeken opgeborgen in een afgesloten kast.
5. De technisch beheerder meldt de technische bijzonderheden aan de beheerder.
6. Jaarlijks wordt door de beheerder gerapporteerd aan het College van Bestuur, volgens het model rapportageformulier zoals in de bijlage. Op verzoek wordt het incidentenregister en logboek ter inzage aan het CvB aangeboden.

Artikel 7. Integriteit, privacy en rechten van de geregistreerde
1. De persoonsregistratie wordt uitsluitend gebruikt conform de doelstellingen van het cameratoezicht.
2. Het cameratoezicht wordt kenbaar gemaakt door middel van borden of daartoe gebruikelijke stickers bij de toegangswegen. Het betreft informatie als “Voor uw en onze veiligheid...” of woorden van soortgelijke strekking.
3. De beeldregistratie wordt maximaal 4 weken bewaard waarna de informatie wordt gewist.
4. Onbevoegden hebben geen toegang tot het camerasysteem.
5. De onder 5.1 genoemde medewerkers gaan vertrouwelijk en integer om met de kennis die zij tot zich krijgen met het cameratoezicht, in het bijzonder met betrekking tot de privacy van derden.

6. Medewerkers die niet onder de CAO van de Hogeschool Utrecht vallen dienen een geheimhoudingsverklaring te tekenen.

Artikel 8. Uitgifte van beeldinformatie

1. Beeldinformatie wordt verstrekt op vordering van de politie of de officier van justitie.
2. De beeldinformatie aan de politie wordt op CD-ROM of andere digitale wijze verstrekt.
3. De politiefunctionaris of de officier legitimeert zich vooraf ten overstaan van de technisch beheerder of bij zijn/haar afwezigheid bij de beheerder of diens vervanger.
4. De media met beeldinformatie die aan de politie wordt verstrekt wordt gemerkt en in het logboek geregistreerd door de technisch beheerder.
5. De politiefunctionaris dan wel de officier van justitie tekent voor ontvangst.

Artikel 9. Inzagerecht beeldinformatie van derden

1. Gelet op de bescherming van de privacy gelden wettelijke beperkingen voor het inzagerecht van derden.
2. Het recht op inzage kan worden verleend als een zwaarwegend belang is aangetoond. De beoordeling hiervan geschiedt door de beheerder.
3. Een verzoek tot inzage van een advocaat, in het kader van een strafproces ter verdediging van een verdachte cliënt, wordt gedaan door tussenkomst van de officier van justitie.
4. Niet-justitiële verzoeken tot inzage worden gericht aan de beheerder.
5. De verzoeker dient zich, ter vaststelling van zijn identiteit, in persoon te vervoegen bij de beheerder of diens vervanger.
6. De beheerder of diens vervanger beslist na weging van de belangen binnen twee werkdagen op de aanvraag.
7. Personen die inzage in beeldinformatie krijgen tekenen een inzageverklaring.

Artikel 10 Toezicht

1. De functionaris voor de gegevensbescherming (FG-p) van de hogeschool voert de controle uit op de naleving van de in dit reglement opgenomen bepalingen.
2. Deze controle omvat het nagaan of de opzet van de organisatie, met inbegrip van de procedures, in overeenstemming is met het gestelde in dit reglement en het nagaan, op willekeurige tijdstippen, of door de desbetreffende functionarissen dit reglement en de procedures worden nageleefd. De controle betreft ook de beveiliging tegen inbraak en diefstal.
3. De FG-p wordt benoemd door het College van Bestuur, die daartoe ook een taakomschrijving voor de FG vaststelt.
4. De FG-p rapporteert ten minste eenmaal per jaar zijn bevindingen aan het College van bestuur, dat het verslag doorstuurt naar de Centrale Medezeggenschapsraad en de Facultaire Medezeggenschapsraden.

Artikel 11 Overgangs- en slotbepalingen

1. De Hogeschool Utrecht behoudt zich het recht voor dit Reglement te allen tijde te wijzigen. Betrokkenen zullen altijd worden geïnformeerd over deze wijzigingen.
2. Onverminderd eventuele wettelijke bepalingen is dit reglement van kracht gedurende de gehele loop-tijd van de registratie.

3. In geval van overdracht of overgang van de registratie naar een andere verantwoordelijke dient de betrokkene van dit feit in kennis te worden gesteld, opdat tegen overdracht of overgang van op hun persoon betrekking hebbende gegevens bezwaar kan worden gemaakt.