

**CAMERA SURVEILLANCE REGULATIONS**  
**OF**  
**WAGENINGEN UNIVERSITY & RESEARCH**

These regulations describe the functions, responsibilities and procedures of the camera surveillance on the premises and within the buildings of Wageningen University & Research (WUR), having regard to the careful use of the camera system and the protection of privacy.

The cameras are able to film constantly and permanently. The images, directed partly by movement detection, are stored digitally. This digital store of images constitutes the processing of personal data as defined by the Dutch Personal Data Protection Act (*Wet Bescherming Persoonsgegevens*). Where there is camera surveillance on the premises and within the buildings of WUR, it is carried out in accordance with the relevant regulations.

### **Article 1. Purpose of camera surveillance**

Camera surveillance is undertaken only:

- a. to safeguard the health and safety of any natural persons
- b. to secure the access to buildings and premises
- c. to protect property in buildings or on the premises
- d. to record incidents
- e. to regulate the traffic flow of visitors to, and staff and students of, WUR.

### **Article 2. Definitions**

1. camera system: the entire system of the cameras, monitors, recording equipment, junction boxes, fibre-optic cables and connectors;
2. video observation room: the room within the images can be watched live and which contains the recording equipment;
3. reception area: space in the building covered by camera surveillance from which images can be viewed during the building's opening hours.
4. images: film images received and recorded by the camera system. The term "images" is included within the term "processing of personal data" as defined by the law;
5. responsible party: the camera system owner, namely the Executive Board of WUR (Wageningen University & Research), represented by the Head of Security;
6. Wageningen University & Research: Wageningen University and the foundation: Stichting Wageningen Research;
7. management: the ensuring of the continuity of the camera surveillance;
8. manager: the staff member of WUR appointed by the Facilities and Services Director or by the operational director of a group within the organisation, responsible for the management of the camera system;
9. operational management: the ensuring of the operation of the camera system;
10. technical management: the ensuring of the technical operation of the camera system;
11. technical manager: the staff member appointed by the manager, responsible for the technical management and/or the outside company that performs the technical management on the instructions of the manager;
12. operational manager: the staff member appointed by the manager, responsible for the operational management;
13. incident: an identified behaviour, disruption, accident or other circumstance that threatens good order, property, health or safety.

### **Article 3. Tasks and responsibilities**

20160905 CG&LS

Update of version 20120802 regarding change of name Wageningen University & Research

**These regulations will be changed in the academic year 2016-2017**

1. Camera surveillance is the responsibility of the Executive Board of WUR, the owner of the camera system.
2. The management of and tasks relating to camera surveillance are assigned to the manager.
3. The technical management of camera surveillance is carried out by the technical manager under the responsibility of the manager.
4. The operational management of camera surveillance is carried out by the operational manager, under the responsibility of the manager.
5. The operational manager will report any incident to the relevant bodies (police, fire services, urgent medical assistance (ambulance) and/or in-house emergency and first-aid service) and to the manager.

#### **Article 4. The video observation room**

1. The video observation room is located in the buildings of WUR where camera surveillance is undertaken.
2. Images are stored and may be looked at in rooms that are protected against burglary and vandalism.
3. The rooms referred to in section 2, above, are only accessible with the permission of the manager.
4. Investigating officers are only allowed access to the rooms referred to in section 2, above, in accordance with the procedure set out in Article 8 and only for the purpose of performing their statutory duties.

#### **Article 5. Operating the camera system**

1. The persons authorised to operate the camera system and/or to examine images are:
  - those responsible for, or supervising, the camera surveillance or who are otherwise necessarily involved in this, including the technical managers, operational managers and the manager;
  - the Director Facilities and Services, the Director of the organisational unit where the camera surveillance is undertaken;
  - the responsible party;
  - third parties (supplier and maintenance provider for the system), if this is necessary for its proper functioning and only with the consent of the manager;
  - police officers, insofar as this is necessary for the proper performance of their public law tasks, or the tasks requested by WUR.
2. During opening hours, camera images may also be looked at in and around their locations by reception staff – employees of the security firm – working in the relevant building. Outside opening hours, they may be looked at by the control centre, security firm, manager, or such other persons designated by the manager.
3. If an incident occurs, it will be reported by the operational manager to the relevant bodies (police, fire services, urgent medical assistance (ambulance) or in-house emergency and first-aid service) and to the manager.
4. Operation of the equipment also includes looking back at digital recordings and the storing of the images on hard disk, CD/DVD-ROM or other means of data transport.
5. Persons who as part of their jobs look at live pictures or operate the camera system must first prove their identities to the manager or operational manager.

#### **Article 6. Reporting**

1. The operational manager must report the use of the camera system in a logbook.
2. This logbook is confidential.
3. The logbook must include the name of the operational manager on duty, the date and time, and notable events, such as breakdowns, incidents, reports, requests for images etc.
4. The operational manager must store the logbook when not in use in a locked cupboard.

5. Every quarter, the operational manager will provide the Facilities and Services Director with a report on the findings, the use of the logbook, the findings regarding registration and consultation of the material.
7. The technical manager must report any technical details to the manager.
8. The manager is accountable to the Facilities and Services Director or the Operational Director of the section of the organisation.
9. The Facilities and Services Director or the Operational Director will report annually to the Executive Board.

**Article 7. Integrity, privacy and rights pertaining to stored images**

1. The stored images will be used only for the purposes of camera surveillance as specified in Article 1.
2. Notice of camera surveillance is given by signage on the premises and in the entrances to buildings of WUR.
3. The images will be stored for a maximum of seven days before being erased.
4. If an incident occurs or if a request is made to view images, the relevant images will be stored for as long as is necessary to deal properly with the incident or the request.
5. Only persons authorised by these regulations have access to the camera system.
6. The camera system is electronically secured against unauthorised use.
7. The officers referred to in Article 5.1 must deal carefully and in confidence with the information they obtain via camera surveillance, especially having regard to the protection of privacy of third parties.

**Article 8. Issue of images to police officers or public prosecutors**

1. Images will only be supplied by order of the police or public prosecutor if there is a legal basis for such request.
2. The images will be supplied digitally, on a CD-ROM or otherwise.
3. The police officer or public prosecutor must prove his identity in advance to the manager, or in his absence to the operational manager, and prove his authority to request the information.
4. A CD-ROM on which images are stored will be marked and recorded by the manager or operational manager. The manager will keep a copy of the images supplied.
5. The police officer or public prosecutor will sign to acknowledge receipt.

**Article 9. Right to examine images of third parties**

1. Third parties, which term includes persons whose images have been recorded, only have the right to examine the images if express consent has been given for this by all relevant parties whose images have also been recorded on the requested images or if permission is otherwise granted pursuant to the Personal Data Protection Act.
2. The right to examine can only be granted if the applicant can prove to have an interest that outweighs other justified interests.
4. An application to examine must be filed in writing with the board for the organisational section to which the building belongs or to the Executive Board of Wageningen University and Research within seven days of the images being recorded.
5. The applicant must prove his identity to the manager or operational manager by means of a legally recognised proof of identity.
6. The applicant will receive by return information about the body which will decide on his application. The images will be stored pending determination of the application.
7. The body referred to in the previous section will notify the applicant in writing of its decision as soon as possible and in any event within four weeks of receipt of the application.
8. Persons who are allowed to examine images by virtue of this article will sign a statement to that effect.

**Article 10. Complaints**

1. Any complaint about the operating of the camera system, the conduct of any staff involved in the camera surveillance, or any application based on the other rights

20160905 CG&LS

Update of version 20120802 regarding change of name Wageningen University & Research

**These regulations will be changed in the academic year 2016-2017**

conferred on relevant parties by the Personal data Protection Act may be submitted in writing to the board for the section of the organisation to which the building belongs or to the Executive Board, Droevendaalsesteeg 4, (6708 PB) Wageningen within six weeks of the recording of the relevant images. A complainant or applicant should take account of the period for which the images are stored. The relevant images will only be stored for the purposes of dealing with the complaint or application if a request is made for this purpose within the storage period of seven days.

2. A complaint or application will be dealt with in the manner described in Article 9 sections 5 to 8.

**Article 11. Notification of camera surveillance to the Dutch DPA**

Wageningen University and Research will notify the Dutch DPA ("Autoriteit Persoonsgegevens") of the processing of personal data in connection with the digital storage of images and their storage period of seven days.

**Article 12. Final provisions**

These regulations replace all previous regulations concerning camera surveillance; they may be cited as the "Camera Surveillance Regulations of Wageningen University & Research".

The regulations have been approved by the relevant participational bodies and were adopted on 14 September 2009.