Guidelines for CCTV surveillance and use of logfiles for electronic access

1. Background and purpose

These guidelines apply to employees and students and specify when and how CCTV surveillance or the use of logfiles can be used at the University. The University wishes to point out that this in no way indicates a desire for general surveillance of employees, students or visitors.

2. Dealing with CCTV recordings, logfiles, etc.

a) If electronic access control, including CCTV surveillance or logfiles, are introduced to prevent or identify criminal activity, data processing must be notified to the Data Inspectorate in accordance with current regulations.[1]
b) Management are to ensure that material cannot come into the possession of a third party.
c) Sound must not be recorded as part of CCTV surveillance unless the employees/students concerned have consented to this.

Reference is also made to legislation in this area, including the Prohibition of CCTV Surveillance Act, Personal Data Act, Penal Code, any contractual commitments and the rules set by the Data Inspectorate.

3. When and where CCTV surveillance and logfiles may be used

3.1 CCTV surveillance

a) CCTV surveillance may only be undertaken subject to an objective, pre-determined purpose, cf. Sec. 6.
b) CCTV surveillance may only be undertaken if there are serious reasons for making this type of surveillance. Only in exceptional circumstances can individual cases of left, vandalism, harassment or the like justify the introduction of CCTV surveillance.
c) CCTV recordings, etc., must not be used for other personal identification purposes than those stated.
d) CCTV surveillance or other access control must not be offensive or cause unnecessary inconvenience to employees and students.
e) CCTV surveillance is not to be used to check on the performance or working hours of personnel or the time they arrive at work.

[1] Processing shall be taken to mean "any operation or series of operations with or without the use of electronic data processing to which data is subjected." S. 2 Personal Data Processing Act.

3.2 Logfiles

a) Logfiles for use in access control must only be used for their designated purpose which would normally be to record incoming and outgoing traffic in a building. Such logfiles may be used where criminal conduct is suspected and on suspicion of contravention of the guidelines for access to buildings.
b) If logfiles are to be used for example for counting the number of people moving around the University's buildings, counting and publication of figures must be anonymised.
c) CCTV surveillance is not to be used to check on employees' performance, their working hours or the time they arrive at work.

4. Notification and signage for CCTV surveillance

a) Signage or other information must clearly state that CCTV surveillance is in progress and where this is happening.
b) Where CCTV surveillance is being done in places where only employees and specially authorised students have access, the requirement for information may be complied with by informing those concerned in writing. Proof of receipt is to be retained. Routines are to be set up to ensure that new employees and new students are duly informed.
c) The signage/information must reflect the area actually under surveillance.
d) Only the police can implement CCTV surveillance without prior signage or information to employees and students in accordance with the *Prohibition of CCTV Surveillance Act.*[2]

5. Managers' role

Ultimate responsibility for CCTV surveillance and the use of logfiles at the University rests with management.
The manager of the area in which there are plans to introduce CCTV surveillance or logfiles is to involve the coordination committee and ensure that the committee gets the information its needs (see below). If management subsequently decides to introduce control systems as previously notified, the employees /students affected are to be duly informed before implementation.
The manager is to ensure that material cannot come into the possession of a third party.

6. Role of the Coordination and Occupational Health Committees

The relevant coordination committee and occupational health committee are to be consulted when there is a plan to introduce CCTV surveillance or logfiles or when there are changes to location or use.
In very special instances, CCTV surveillance or logfiles may be used without prior discussion by the coordination/occupational health committees and without notifying employees for students. This would be on suspicion of the law being broken which could lead to the police being involved and where unless surveillance were immediately started, the opportunity for identification would be lost. It should be noted however that only the police can undertake CTV surveillance without prior signage, etc., cf. Sec 4d. In such a situation, an employee representative such as the deputy chairman of the coordination committee, or a union representative for the group of employees concerned, is to be

[2] Act 1190 of 11/10 2007 Statutory Instrument on the CCTV Surveillance Act (https://www.retsinformation.dk/Forms/R0710.aspx?id=105112&exp=1) – In Danish

involved. If CCTV surveillance or logfiles are introduced where there is access for students, the matter is further to be discussed with student representatives in the occupational health committee, or if there is none, with student representatives on the Academic Council. The coordination committee and the occupational health committee, students and employees affected must in any event be notified when the specific surveillance has been completed.

The manager must give details of the following for use in discussions with the coordination /occupational health committees:

a) The whole purpose of CCTV surveillance and/or logfiles.
b) Who has the right to review the material and the circumstances in which this will be done, such as by way of random sampling, on definite suspicion or something else.
c) The extent to which employees and students are entitled to access data about themselves and have the right to object and to complain for example to the Data Inspectorate.
d) A plan for how present and future employees and students are to be informed of surveillance and the conditions under which this would happen, including how long data/recordings are to be kept.
e) The situations in which material might be passed to the police.

7. Validity and termination

The guidelines shall take effect on adoption by HSU.

Termination must comply with the rules in the coordination committee's circular according to which either of the parties can give three months notice of termination of the established guidelines. Before termination, the coordination committee is to endeavour to amend the present guidelines so as to make them satisfactory for the parties in the coordination committee.

Considered and adopted at the HSU meeting on 24 June 2009.

Ralf Hemmingsen
Rector and Chairman of the
General Collaboration Committee

and

Poul Erik Krogshave
Deputy Chairman of the
General Collaboration Committee

Representatives of the students whom it is assumed would be involved if the guidelines were to be significantly amended have signed up to the guidelines.

Other references:
Relevant provisions in the Personal Data Processing Act and the Penal Code. Link to the Personal Data Processing Act (Danish): https://www.retsinformation.dk/Forms/R0710.aspx?id=828
Link to the Penal Code (Danish):
https://www.retsinformation.dk/Forms/R0710.aspx?id=113401
Any contractual commitments and the rules laid down by the (Danish) Data Inspectorate