



SWEDISH POLICE REQUIREMENTS FOR CAMERA SURVEILLANCE SYSTEMS



This document offers guidelines for users of camera surveillance systems, where the recorded images are intended to be used by the police and other parts of the legal system to discover, investigate and prosecute crimes. For good results, the system should fulfil fundamental requirements regarding:

QUALITY – is the image content accurate, and is the visual quality sufficiently good?

SECURITY – is the image material managed in a secure manner?

ACCESSIBILITY – can the police quickly and simply access and manage the pictures?

By ensuring that your camera surveillance system satisfies a few fundamental requirements, the potential value of the images as evidence increases tremendously. A few points that your system should satisfy are presented below. More detailed explanations of these recommendations are given overleaf.

QUALITY Security needs – Checks – Image quality – Image content – Image rate

1. Specify your security needs and appoint the purpose of the system – what do you want to see and where.
2. Check your system – review the pictures from the system's removable medium, not the pictures shown directly on the screen, and check that you can see what you have specified.
3. Conduct regular inspections – ensure that you have, and follow, an inspection schedule adapted to your system.
4. Factors with a big influence on picture quality are:
 - Camera placement: The camera's height, direction, distance and how discreet it is, are crucial for the results.
 - Lighting: Even lighting gives the best images. Back-lighting and point lighting considerably worsens the visual quality.
 - Compression: Compression can erase vital details from the images – increase instead the memory capacity.
 - Resolution: As higher resolution as more details in the images – this is important, particularly for close-up cameras.
 - There should be one camera per surveillance task, so differentiate between wide-angle cameras and close-up cameras.
5. Image rate – is it sufficient for the camera's surveillance purpose? Will the course of events and close-up images be captured?

SECURITY Personal integrity – Value as evidence – Reliable

1. Recording equipment and stored audio and image material must be locked in.
2. Only authorized and educated personal may have access to recorded material. It is covered by professional security.
3. Text information with time/date and camera ID must be burned into the images.
4. There should be a checklist for what is to be done when an incident occurs. Important issues are,
 - Check the time and date in the system against the Speaking Clock, and record any deviation.
 - Save all recorded material on a removable medium.
 - Make image material read-only, and label.
 - When image/audio material is transferred, evidence of the transfer should be signed by the issuer and recipient.

ACCESSIBILITY Exporting – Image/audio format – Media player

1. Locks, physical or electronic in the form of passwords or encryption, must not prevent authorised persons from quickly gaining access to recorded material after an incident.
2. The system must provide a suitably removable medium, such as VHS tape, CD/DVDs, or removable disk.
3. A *simple manual* must be kept by the recording equipment, explaining how the visual material is to be exported.
4. The visual material must be exported without lowering the quality.
5. Information about visual/audio format, the number of cameras, image frequencies, and a plan of the surveillance area showing camera placement, must be supplied with the visual material.
6. Together with digital visual material, an associated media player must be supplied. The media player must be able to
 - Distinguish between and play each camera individually, in real rate and at full resolution.
 - Quickly arrive at the sequence in question.
 - Progress frame by frame.
 - Export still pictures (sequences of still pictures) to uncompressed standard format.
 - Manage sound (if it is recorded).



SWEDISH POLICE REQUIREMENTS FOR CAMERA SURVEILLANCE SYSTEMS



COMMENTS:

QUALITY

1. It is very important that the user of a camera surveillance system has a clear understanding of the aim of the system. Specify what is to be captured, what is to be seen and where. Examples are recognising the faces of people passing the entrance, reading the number plate of a vehicle at the petrol pump, or checking the transaction at the cash desk. Often you want answers to the questions *What happened?* and *Who did it?* Both wide-angle cameras and close-up cameras are then needed. Always try to attain the highest possible quality. If the choice is between higher quality or longer recording time – always choose the higher quality.
2. A good way of testing whether a system satisfies the established requirements is to conduct a practical test. Ask someone to perform some action in front of the camera or park a car in the place under surveillance. This should be done under the same conditions as those for which the system is intended. Then transfer the visual material to the system's removable medium. Check the pictures from this medium, rather than those displayed directly on the screen. What is interesting is the quality of the pictures delivered by the system. Is it possible to see the objects specified in the requirements? If you can't see something, there is generally nothing more that can be done. So – *Test your system before the criminal does!*
3. Regular inspections are the only way to see if the system is working and recording images of sufficient quality.
4. Camera placement should preferably be close, directly forwards, and at the same height as the object you under surveillance in order to get the best visual quality. At the same time, it should be difficult for the criminal to cover, break or redirect the cameras. Use concealed cameras, misleading imitations, etc. When placing the cameras, it is also important to consider the lighting conditions in the room in the form of artificial lighting and windows.
Lighting conditions should be even, preferably with some front lighting, and sufficient for the system in question. Point lighting, such as spotlights and back lighting, often from windows, can cause shadows that erase important information in the images, thereby making it impossible to identify objects or people. Compressing is used in order to store more pictures on a limited storage unit. This is done at the expense of details being erased from the stored pictures. Compressing should therefore be used with the utmost caution to avoid erasure of details that may be critical for a criminal investigation. The details comprise the individual characteristics that are necessary for recognition and identification of objects and people.
5. The image frequency required depends on what the system is intended to capture on film. Is it sufficient to record that someone/something has moved in area under surveillance, or is the system to document detailed movements? If the camera's task is identification, the high image frequency is required when the object in question passes the camera, but otherwise a lower image frequency is sufficient. This can be regulated using movement detection.

SECURITY

1. To protect personal integrity, and to prevent sabotage, the recording equipment and visual material must be kept in a locked facility. The room or cupboard should not have a sign to indicate that it contains surveillance equipment. Keep a logbook about what is done with the system and by whom.
3. To identify the images, the time/date and the camera ID should be burned onto the images. To reduce the risk of errors, the system should be provided with automatic synchronisation of the time/date with an external source.
4. If no other agreement is made, all stored visual material must be exported to a read-only removable medium. Label the medium with the title, time and date of the medium. The person who exported the visual material should sign the medium. If possible, place it in a sealed deposit bag.

ACCESSIBILITY

1. Keep information by the recording equipment about who is to be contacted if help is needed. When the visual material has been exported to the removable medium, it must not be locked with an electronic lock such as a password or encryption because this can make it difficult for the police to handle it.
2. If the system lacks a removable medium to which the desired visual and audio material can be exported without loss of quality, the police may be forced to take all the recording equipment.
3. A person who has not previously used the system must be able to follow instructions in the manual to export visual material from a desired time interval.
4. There should be no format conversion, compressing or any other activity that lowers the image quality when the visual material is exported.
5. A plan of the surveillance area should be supplemented with a test image from every camera.
6. Necessary software must accompany the digital material to guarantee efficient handling by the authorities in question. The media player must give information about resolution, colour format, compression method, image frequency, storage format, etc.