RISK MANAGEMENT GUIDELINES
CCTV and the Data Protection Act

Introduction
The position of a CCTV system in relation to privacy was uncertain up to the publication in March 2000 of a Code of Practice to the Data Protection Act 1998. This brought systematic legal control to the area and established beyond doubt that most security applications of CCTV are subject to the same legally enforceable requirements as other forms of electronic data processing.

Owners of any technical system used for "processing" defined by material namely "personal data" must notify (register) their operation to the Information Commissioner and ensure they are in compliance with the Data Protection Act. In addition, public bodies must have regard to the requirements of the Human Rights Act 1998.

Subject Rights
Data Subjects (in this context, persons whose images have been captured by the CCTV system) have the right to view or be given a recording of the video sequence in which they are captured. This is termed Subject Access. They are also entitled to require that the Data Controller ceases video processing which might cause unwarranted damage or distress. Furthermore, if an automatic decision taking facility is in use (e.g. number plate or facial recognition system), the Data Subject is entitled to notification if no human intervention is involved in the decision. If an automatic decision has a significant effect on the Data Subject, he is entitled to appeal against it. This might occur, for example, in the field of employee relations (e.g. time keeping).

Key Requirements of the Act
The Code of Practice contains mandatory requirements and also recommendations for good practice. It is import to recognise however that the Information Commissioner will take into account the extent to which users have complied with the totality of the Code when determining whether the legal obligations have been met.

Mandatory Requirements
• Notification under the 1998 Act is mandatory whether or not a storage device (recording facility) is included. Furthermore the requirements are not limited to systems viewing areas to which the public have access.
• All systems that capture pictures of individuals (including employees) other than the Data Controller himself are subject to the Act. (A system installed in his own residence by the owner is, however, not required to be notified to the commissioner). Similar surveillance devices such as audio systems and, possibly 35mm surveillance cameras, are included.
• The owner must identify a person to take responsibility for the system and establish its purpose and rationale.
• Cameras should not be allowed to view places not covered by the "purpose" but if there is a possibility that they could capture scenes of neighboring domestic premises, the user must consult those neighbors.
• The CCTV operator(s) must be instructed to apply the system only in line with the stated purpose and, if necessary, adequately trained in privacy policy.
• Signs to warn the public that they are entering a zone covered by CCTV must be erected and the sign must include the identity of the responsible person or organisation complete with contact details. If the sign does not show a symbol of a camera, the purpose of the system (e.g. "prevention and detection of crime") must also be stated on the sign.
• The signs must be of adequate size e.g. A4 for pedestrian traffic, A3 for vehicular traffic.
• There are stringent conditions covering the use of covert cameras (i.e. cameras used without signage) which must not be used unless there is specific criminal activity to be detected and then only for as long as is necessary to capture the relevant evidence.
The equipment must:

- work accurately and be checked out for correct operation
- be properly maintained and protected from vandalism
- be repaired promptly when defective
- operate in suitable conditions (e.g. adequate lighting).

• Only good quality tapes, erased before every session, should be used and they should be renewed after 13 recording sessions.

• If the “purpose” includes the apprehension and/or prosecution of offenders, then the system must be capable of capturing images that allow identification of individuals.
• Elements that can make automated decisions such as facial recognition systems must not operate without human intervention.
• Unnecessary recording should be avoided and recordings should be disposed of/wiped after a reasonable time (e.g. 31 days at the most).
• Retained recordings and CCTV monitoring must be subject to access control and appropriately secured against unauthorised disclosure.
• Proper records must be kept of any recordings that are viewed or disclosed.
• Only designated, properly trained staff should operate the system and view images.
• All staff must be aware of the owners privacy and disclosure policy and Data Subjects
The owner must provide an application form and explanatory leaflet to Data Subjects wishing to view or obtain a recording of their images. The application must be satisfied within 40 days against a fee not exceeding £10. A contact point must be available to the public during office hours.
• There must be a written contract with any third party Data Processor containing details of the Data Processor’s security guarantees.
• The owner must carry out a review of the system and its procedures at regular intervals.

Good Practice
The code contains a number of recommendations for good practice, which fall mainly in the area of documentation and records and the need to keep the system and procedures under continuous review.
• Obtain a copy of the Code of Practice from the Information Commissions web site at www.dataprotection.gov.uk.
• Avoid recording what is not absolutely necessary and dispose of recordings in the shortest practicable time.
• Ensure when designing systems that monitors are not in the view of unauthorised people and that stored recorded material and recording equipment are under lock and key.
• If there is a CCTV operators’ room it should be subject to access control.
• Fixed cameras should not be allowed to capture images of private property. If necessary, elements of the captured image can be blanked off using digital masking. It may be possible to restrict the travel of PTZ cameras to avoid capturing such images. Failing that, steps must be taken to properly instruct and supervise the system operators.
• Security firms can supply complete suites of appropriate documentation, logs, signage, tape, cabinets, VCR cages etc. This considerably eases the task of complying with the many and varied requirements of the Code

Note:
Due to a recent court case it appears that most of the previous requirements to notify the Information Commissioner if an Assured installed CCTV and to pay a fee no longer apply. The Information Commissioner was very unhappy with the court verdict but it is our understanding there has been no appeal. Accordingly it is worth checking with the Information Commissioner to check how much of the above is still relevant.