Code of Practice for Digital Recording Systems for the Purpose of Image Export to be used as Evidence

ISSUE 1

OCTOBER 2005

BSIA Form No. 191

© This document is the copyright of the BSIA and is not to be reproduced without the written consent of the copyright owner
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>2</td>
</tr>
<tr>
<td>1 Scope</td>
<td>2</td>
</tr>
<tr>
<td>2 Normative references</td>
<td>2</td>
</tr>
<tr>
<td>3 Abbreviations</td>
<td>3</td>
</tr>
<tr>
<td>4 Terms and definitions</td>
<td>3</td>
</tr>
<tr>
<td>5 Image quality</td>
<td>5</td>
</tr>
<tr>
<td>6 Admissibility as evidence</td>
<td>6</td>
</tr>
<tr>
<td>7 Audit trail</td>
<td>6</td>
</tr>
<tr>
<td>8 Image authenticity</td>
<td>7</td>
</tr>
<tr>
<td>9 Storage</td>
<td>7</td>
</tr>
<tr>
<td>10 Export of images</td>
<td>8</td>
</tr>
<tr>
<td>11 Playback of exported images</td>
<td>10</td>
</tr>
<tr>
<td>12 Time and date integrity</td>
<td>10</td>
</tr>
</tbody>
</table>
Introduction
The demand for this code of practice (CoP) is based on the videocassette recorder (VCR) medium in many cases being replaced by digital video recorder (DVR) technology within security applications with the result that end users and specifiers are requesting guidance. The rapid change towards DVR technology is based on improved reliability, ease of use, ability to search for specific recorded data quickly, no need for daily attention, in particular, relating to the constant requirement to change video tapes and the retention thereof. This CoP does not attempt to establish a preference for the digital recording medium to be adopted but does recommend the areas that should be considered when adopting DVR technology.

1 Scope
This CoP has been prepared to assist companies and organisations in the specification, selection, installation and operation of DVR equipment, and systems, for the purpose of closed circuit television (CCTV) images to be used as evidence in a court of law. This document is aimed at assisting specifiers, installers, users, insurance companies, police authorities and purchasing organizations. Particular emphasis is placed on the following key areas:

a) Image Quality
b) Admissibility as evidence
c) Image Authenticity
d) Storage
e) Export of Images
f) Playback
g) Operator / Owner Awareness
h) Audit Trail

2 Normative references
The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

BS EN 50132-7:1996 Alarm systems – CCTV surveillance systems for use in security applications

Digital imaging procedure – Version 1.0 March 2002 PSDB

Code of practice of legal admissibility and evidential weight of information stored electronically - BIP0008.

Digital images as evidence – House of Lords select committee on science and technology session 1997-8 5th Report.

UK Police requirements for digital CCTV systems – Home office/association of chief police officers (ACPO), Publication 09/05.

Data protection act 1998 (DPA)
Information commissioner CCTV code of practice (section 51(3)(b) DPA '98)
3 Abbreviations

CCTV  Closed Circuit Television
CD    Compact Disc
CD-RW  Compact Disc – Read / Write
CoP   Code of Practice
DAT   Digital Audio Tape
DPA   Data Protection Act
DVD   Digital Versatile Disk
DVR   Digital Video Recorder
HOSDB Home Office Scientific Development Branch (formerly PSDB)
IP    Internet Protocol
PC    Personal Computer
PSDB  Police Scientific Development Branch (now known as HOSDB)
RAID  Redundant Array of Independent Disks
SAN   Storage Area Network
VCR   Video Cassette Recorder

4 Terms and definitions
for the purpose of this CoP the following terms and definitions apply:

4.1 audit trail
data which allows the reconstruction of a previous activity, in its correct chronological place, or which enables the attributes of a change (such as date/time, operator) to be recorded

NOTE The list can be generated by a computer system (for computer system transactions) or manually (usually for manual activities)

4.2 authentication
proof that the original recording has not been altered since first writing to storage media and that the master copy is an exact copy of the original recorded digital images

4.3 CCTV camera
a unit containing an imaging device producing a video signal from an optical image

4.4 CCTV system
system consisting of camera equipment, monitoring and associated equipment for transmission and controlling purposes, which might be necessary for the surveillance of a defined secure area

4.5 digital image
image consisting of pixels using ranges of discrete values
4.6 **digital video recorder**
A DVR is a system that is capable of recording, playback and export of digital images captured by CCTV cameras. A DVR may consist of one physical box or could be multiple components, spread across a network.

Examples of components include video/audio capture hardware, input/output interface hardware, processing hardware, storage media and network interface hardware.

4.7 **event**
Incidents recorded on the DVR that could be of interest. Depending on the configuration of the DVR, specific event types may become searchable criteria.

4.8 **event log**
A chronological list of events or operations which have occurred in the DVR.

4.9 **exact copy**
Transfers of digital images from a source (original recording or master copy) to separate digital storage media where the copied image data is a bit-for-bit copy of the source.

4.10 **export**
Transfer of data from the original stored location to an alternative storage location.

4.11 **fit for purpose**
Meets defined operational requirements for the recording and playback of each individual camera.

4.12 **master copy**
An exported exact copy made from the original recording.

4.13 **metadata**
Data about data.

NOTE: For example, the context and relationships of data with other data which is necessary to render that data more understandable.

4.14 **original recording**
First instance of digital images recorded to the DVR’s on-line storage to be used for playback and/or export.
4.15
picture quality
value of the recorded evidence depends upon the picture quality. Picture quality inherently relates to its intended use, it is therefore purely subjective. The final assessment of the played back images should be made against the system specification in terms of ‘fit for purpose’

4.16
playback
viewing of previously recorded images from the DVR

4.17
retention period
specified time for which digital images are to be held on the DVR system’s storage media to meet the purpose of the application

4.18
storage
digital media on which digital images are stored. Examples include hard disk drive (local or remote), digital tape, CD, DVD, flash memory:

a. local: storage media that exists in the same physical box as the majority of the other DVR components. Removable media is included in this category if it is located locally for the purpose of writing original recordings to it

b. external: storage media existing physically separate to other DVR components and connected by a communication link. Examples of external storage include RAID arrays, file servers - PC providing storage, SANs etc

c. on-line: either or a combination of the above which is accessible immediately by the DVR

4.19
working copy
additional copies other than the master copy made either from the original recording (at the same time as the master copy) or from the master copy. The working copy should be an exact copy of the master copy when created. The working copy may be subsequently altered due to processing, e.g. image enhancements

5 Image quality
Before evaluating image quality, ensure that the reason for recording the images is clearly defined and understood. Choose the highest image quality of system as possible, ensuring that the images produced are fit for that purpose.
Always judge the capability of a DVR by the quality, taking the following factors that affect image quality into account:

a) subject size within the field of view of the camera
b) lighting of subjects within field of view
c) camera & lens specification
d) recorded digital image compression  
e) image per second record rate per camera  
f) transmission medium  
g) system maintenance  
h) recorded digital image resolution

NOTE: for further information refer to EN50132-7

6 Admissibility as evidence

6.1 Producing evidence
The House of Lords Select Committee on Science and Technology Session 1997-8 5th Report, states that digital recording technology provides no original that could be produced in evidence. All that is available for use as evidence is a copy of the first, probably temporary, recording in memory, and this will be admissible as evidence.

Its weight and admissibility as evidence will depend on:

a) Whether the image’s audit trail from the digital recording device to the court is robust  
b) whether the integrity of the image can be proven.

It is at the Court’s discretion whether the evidence is deemed admissible.

NOTE 1: Operators of CCTV systems must comply with the legal requirements of the Data Protection Act 1998 (DPA), because failure to do so may result in legal action being taken under this Act.

NOTE 2: for further information refer to the Information Commissioner CCTV code of practice (section 51(3)(b) DPA ’98).

7 Audit trail
The methods of operation and management of the system can affect the admissibility of evidence. Therefore it is important that actions and events for the recording system are logged. The audit trail should cover the period from when the original recorded images are recorded to media to the point which, the police or prosecuting authority take control of the master or evidential copy or it is no longer required.

Note: For further information refer to PSDB’s ‘Digital Imaging Procedure’ – version 1.0, March 2002.

8 Image authenticity
It is important that the integrity of the images from the DVR can be proven, such that the original recorded images and subsequent copies cannot be altered without detection. ‘Digital Watermarking’ is a term commonly used to describe image authentication, however this should not be confused with the Digital Watermarking method described below. Various techniques can be employed to detect image tamper, for example:

a) Digital Fingerprinting  
b) Checksumming  
c) Digital Watermarking
The DVR manufacturer should be capable of providing a statement that can be used in defence of the authentication method employed.

Note: This CoP does not intend to detail all authentication methods since other techniques will be developed in the future. The above listed items are examples of commonly used techniques and these are provided as a guide.

8.1 **Digital fingerprinting**
A method of generating a unique ‘fingerprint’ of the original recorded image that cannot be reproduced if the ‘original recorded’ image is altered and therefore reveals image tamper.

8.2 **Checksumming**
Each image is checksummed according to an algorithm based on unique key data. Any change to the image or metadata would cause a massive change in the resultant checksum.

8.3 **Digital watermarking**
Visible watermarking describes visibly insignificant changes made to the pixel values to incorporate information, which changes if the image file is altered. Originally the primary use of watermarking was to protect the intellectual property rights of the photographer or filmmaker and its use may have lead to claims that the image was not authentic because the pixels had been changed.

Invisible watermarking, a form of checksumming, can provide image authentication checks without compromising the integrity of the original recorded digital image.

9 **Storage**

9.1 **Data encryption**
Data encryption scrambles the digital data that forms an image in such a way that it would be difficult to reconstruct into the original recorded image. A reverse algorithm is required to reconstruct the image. **Data encryption should not prevent authorised users / organisations from gaining access to playback of the exported images.**

9.2 **Security**
It should be demonstrable that access to storage media by either physical or electronic means is sufficiently controlled to prevent unauthorised access. Approved access should be logged to include whom did what and when either via an access control system or via an audit trail.

9.3 **Recording retention**
Careful consideration should be given to how long images are required to be stored prior to specifying a DVR system. Allowance should be made for event discovery through to playback / export by all interested parties. The quality of images should not be compromised to increase storage period.

Note: Many DVR systems overwrite the oldest images when the storage capacity becomes full regardless of the intended retention period. Many DVR systems provide an image protection mechanism which allows a user to manually or automatically protect images from over-write. Care should be taken to ensure that protected images do not use up storage space such that expected overall record durations are comprised.
9.4 Storage functionality
The system must be intuitive and assist the user in management of the system. One of the key features that a user requires is the ability to see how much recording they are receiving on their particular site:

a) the DVR system should indicate how many days and hours of recording the system has stored.
b) the DVR system should indicate an estimated retention period based on the changing of settings.

9.5 Removable storage media
Where removable media is used as primary storage, care is required in how that physical media is utilised. While the removable media exists within the DVR under controlled access, the digital images on that media may be considered as both the Original Recording and master copy.

It should be noted that:

a) should the media be removed for evidential purposes as part of a correctly audited process, then that specific media could be considered as the master copy.
b) if the media is removed or returned without appropriate auditing, then it constitutes an uncontrolled copy, which could reduce its evidential value.

10 Export of images

10.1 Image enhancements
DVRs may provide enhancement tools such as image sharpening, brightening or zooming in on a particular part of the image. Any applied enhancements must not change the ‘original recording’ or ‘master copy’ images. If an enhanced image is exported, an audit trail must exist as defined within the audit trail section of this document.

10.2 Image export
To facilitate replay and export the following should be adhered to:

a) a trained operator and simple user guide should be available locally
b) export of medium and large volumes of data can take a substantial period of time. The operator should know the retention period of the system and approximate times to export small (15 mins), medium (e.g. 24 hrs), large several days (up to all of the system) amounts of data.
c) the software needed to replay the images should be included at export, otherwise viewing by authorised third parties can be hindered.
d) export of a DVR event log, audit trail and any system settings with the images will assist with establishing the integrity of the images and system.
e) the amount of video that an investigator will need to export will be dependent on the nature of the investigation. It is essential that the system is capable of doing this quickly and to an appropriate medium.
f) export and recording should be possible at the same time without affecting the performance of the system.
The system should not apply any compression or format conversion to the image when it is exported from the system, as this can reduce the usefulness of the content.

Export of the original signature i.e. digital fingerprinting, checksumming, digital watermarking should be carried out to ensure image authenticity.

Hardware used for exporting images should be capable of verifying export was successful.

Note: If it is not easy to export the images from a DVR then the Police may remove the DVR from the premises for further investigation.

**10.2.1 Export media**
The export media should be proportionate to the amount of data to be exported.

A number of scenarios exist on how to export images from a DVR:

a) The image is printed from the unit onto some form of paper.
b) The image is copied (locally or remotely) to some form of removable digital media such as a floppy disk, DAT tape, flash card, CD-RW, hard disk, DVD.
c) The removable hard disk, which holds the images, is physically removed from the DVR.
d) The images are played back on the DVR to enable them to be recorded onto a conventional analogue VCR tape.

**10.2.2 Export file format**
Wherever possible the video and audio material should be exported in the DVR’s native file format and should be an exact copy of the original recording / master copy.

**10.2.3 Exporting of supporting data**
The time and date information with any associated metadata should be exported with the relevant images. If the DVR supports event logging and audit trails then the facility for saving the DVR’s settings and its event log/audit trail when exporting material should be provided.

**11 Playback of exported images**
Where the export media is intended to be replayed on a PC, the playback software should:

a) Have variable speed control including frame-by-frame forward and reverse viewing.
b) Display single and multiple cameras and maintain aspect ratio i.e. the same relative height and width.
c) Display a single camera at the maximum record resolution.
d) Permit the recordings from each camera to be searched by time and date.
e) Allow printing and/or saving (e.g. bitmap) of pictures with time and date.
f) Allow for time synchronised multi-screen playback.
g) Allow for time synchronised switching between cameras upon playback.
h) Allow Playback of associated audio and other metadata.

The time and date, and any other information associated with each picture should be legible and should not obscure the image.
12  Time and date integrity

12.1 General
In terms of evidence the time and date information of the system is key. The user should ensure that the time and date (including time zones) is correct and that it is checked regularly.

12.2 Synchronisation
Multiple DVRs should provide a method of time and date synchronisation between the DVRs, either manually or automatically. Daylight saving time changes should also be accommodated by the DVR.