Disclaimer:

As a condition to the use of this document and the information contained herein, the SWGIT requests notification by e-mail before or contemporaneously to the introduction of this document, or any portion thereof, as a marked exhibit offered for or moved into evidence in any judicial, administrative, legislative, or adjudicatory hearing or other proceeding (including discovery proceedings) in the United States or any foreign country. Such notification shall include: 1) the formal name of the proceeding, including docket number or similar identifier; 2) the name and location of the body conducting the hearing or proceeding; 3) the name, mailing address (if available) and contact information of the party offering or moving the document into evidence. Subsequent to the use of this document in a formal proceeding, it is requested that SWGIT be notified as to its use and the outcome of the proceeding. Notifications should be sent to: Chair@swgit.org

Redistribution Policy:

SWGIT grants permission for redistribution and use of all publicly posted documents created by SWGIT, provided that the following conditions are met:

1. Redistributions of documents, or parts of documents, must retain the SWGIT cover page containing the disclaimer.

2. Neither the name of SWGIT, nor the names of its contributors, may be used to endorse or promote products derived from its documents.

Any reference or quote from a SWGIT document must include the version number (or create date) of the document and mention if the document is in a draft status.

Section 24

Best Practices for the Retrieval of Digital Video

Purpose

The purpose of this document is to provide the best methods for the retrieval of video/audio data evidence and any associated metadata (referred to in this document as data) from Digital Closed Circuit Television (DCCTV) recording systems.

These best practices, guidelines and recommendations are intended to provide responding law enforcement personnel guidance in securing and collecting data from DCCTV systems. This will ensure that best methods are utilized to retrieve the recorded data and maintain its integrity.

The retrieved data should be retained as the master evidence. Whenever possible, the native/proprietary recorded data from the DCCTV recording system should be retrieved to maintain the integrity and image quality of the evidence.

These guidelines are meant to inform agencies of the best practices for DCCTV retrieval and to aid in the development of Standard Operating Procedures (SOPs). These practices should be used in conjunction with current agency policies.

Scope

This document is intended to provide procedures for the collection of data that ensure playback while maintaining best evidence. DCCTV retrieval is the collection of relevant data from a digital video recording system. This may not follow the methodology of computer forensics. The key differences between DCCTV retrieval and a computer forensic investigation are that, with DCCTV retrievals the recording device's operational settings may have to be reconfigured to retrieve the data, and the entire system's contents may not require a forensic examination. This document is not intended to address forensic video or audio analysis techniques performed after the retrieval of data. See SWGIT document "*Best Practices for Forensic Video Analysis* "and SWGDE document "*Best Practices for Forensic Audio*" for more information.

Recognizing DCCTV Evidence and its Nature

Due to its value in the evidentiary process, as well as its potential value for intelligence and security matters, it is imperative that Law Enforcement recognize, protect and properly collect data from DCCTV systems.

- DCCTV information may exist at a scene or at adjacent locations
- Look up, look down, and look around
- DCCTV may be recorded or stored at a remote off-site location

Types of Digital Video Recording Systems (DVRs)

DCCTV systems primarily found in residential, commercial or governmental institutions include two major types:

- Stand-Alone Embedded Digital Video Recorder
- Personal Computer

Stand-Alone Embedded Digital Video Recorder – menu-driven device containing a recording system that typically uses a non-traditional operating system.

PC-Based Digital Video Recorder – may appear to be a standard computer or may be a proprietary turnkey system with video recording capability.

Both systems may have the following:

- Built-in multiplexer
- Transactional data
- Audio recording capabilities
- Other peripheral devices as part of the system
- Network capabilities
- Camera control capabilities
- PC-based systems may also contain business and/or personal data

DVR Recordings

All DVRs utilize compression when recording data to reduce the amount of storage and transmission requirements. Most digital video recording systems utilize a proprietary native file format to record data. This usually requires proprietary playback software or a special codec from the manufacturer to play back the files and any metadata (e.g., time, date, camera number).

In addition to the retrieval of the native/proprietary video files, many systems allow the data to be downloaded/exported in an "open file format" that will be viewable in a non-proprietary software (e.g., AVI in Windows Media Player or MOV in QuickTime). It should be taken into consideration that these methods often further compress the video data.

Whenever possible, the native/proprietary recorded video file(s) from the DCCTV recording system should be retrieved to maintain the integrity and image quality of the evidence. In addition, consideration should be given to retrieving a non-proprietary video file to facilitate quick viewing.

Steps To Take Upon Scene Arrival

- Notes should be kept detailing the methods used and steps taken.

- Determine if a manual is available to assist with system information (e.g., passwords, output options).

- Establish that relevant video has been recorded by reviewing the recording. Preferably, a person with knowledge of the recording device should operate it during playback, if it is appropriate for them to do so.

- Determine the earliest recorded date. This will determine approximately how much time you have to retrieve the data before the system overwrites it.

    - For example, if the earliest recorded date is seven days prior to the incident date, you may have no more than seven days before the relevant data is written over.

- Determine if retrieval can be performed by the venue owner/security system's operator. If yes, will it be in line with best practices?

- Determine if the DCCTV installer company or a trained operator is available to assist in the retrieval.

- Compare the time displayed by the DCCTV system with the current time. Document the difference, if any. It is suggested that a reference clock be used, such as the Navy Observatory Master Clock at (202) 762-1401 and (202) 762-1069, or NIST Telephone Time of Day Service at (303) 499-7111. These services will provide Universal Time and/or Eastern Time.

- Acquire and document the following information:

    - Digital video recorder make, model and serial number

    - Whether system is PC-based or Stand-Alone Embedded

    - Number of recording units installed

    - Whether system is networked

    - System time and date displayed

    - Actual current date and time (from reference clock)

    - Recording capacity of the system and when it will overwrite

    - Number of camera(s) and the active camera numbers

    - Camera(s) make and model

    - Are any cameras infrared-sensitive and, if so, identify.

    - Is audio being recorded? If so, how many channels and are they all downloadable/exportable?

- Multiplexer make and model, if applicable
- Device and/or operating system password
- System settings
    - Image quality (e.g., high, medium, low)
    - Frames/pictures per second
    - Recorded image/frame size (e.g., 320 x 240)
    - Can it be determined if any cameras are alarm or motion triggered?
    - Number of hard drives; storage capacity of each
    - System firmware version
    - Other available system settings (e.g., event log, passwords)
- Playback software password
- Playback software name and version
- Is a copy of the most current maintenance/service log available or obtainable?
- Other information of importance
- Scene contact information
    - Scene address
    - Hours of operation
    - Scene point of contact (with access to DVR) and telephone number
    - DCCTV system installer point of contact and telephone number

- Photograph system (front and back).
- Sketch DCCTV camera placement and position (See Appendix A).
- Remove network cable, if necessary.
- Determine how much data needs to be retrieved.
- Determine the native/proprietary file format the system uses.
- Determine best method for retrieval.

Assessing the Recording System for Output

A determination should be made as to how much and what type of data needs to be retrieved from the DCCTV recording device. An evaluation of the output options of the system should help determine the best and most practical method. When making this assessment, collection of the native/proprietary video file(s) should remain the highest priority to ensure image quality. Other factors to consider include: the amount of media required, law enforcement hours that will be incurred, and the data transfer time.

Examples:

If the incident is a 10-minute robbery, the system has a CD writer and the proprietary file(s) fit on a CD, then collection on CD would be the best method.

If the request is for 24 hours of video and the system has an external USB port, connecting an external USB hard drive may be the best option. This assumes that the system allows for recovery of large amounts of data at one time.

If the request is for 30 days of video, the best, or only, option may be producing a forensic clone of the hard drive(s) and/or removing the recording unit from the scene. See SWGIT document "*Best Practices for the Analysis of Digital Video Recorders*".

DVR Recording System Outputs (systems may include more than one)

This list is not exhaustive and other methods may exist based on the recording system.

- Optical Disc (e.g. CD-R/DVD-R, CD-RW/DVD-RW, Blu-ray)
- Flash media (e.g. Compact flash (CF), Secure Digital (SD))
- USB (1.0, 2.0 and 3.0)
- IEEE 1394 Firewire/iLink
- eSATA
- Network port
- Analog video (RCA, S-Video, Composite)
- VGA/DVI/HDMI output
- SCSI port (50 pin and 60 pin)
- Removable hard drive
- Magnetic digital data storage tape (DAT, DLT, DDS, AIT)
- DV cassette drive (e.g. Sony HSR-1P)
- Iomega Jaz
- Iomega Zip
- Magneto Optical

Important:

- Administrative and/or engineer login access to the DVR usually allows more options for retrieval, including native/proprietary files.

- Time/date stamp with file. You may have to take the downloaded/exported file without the time/date data to ensure the highest quality footage, and take a second retrieval of the footage which includes the time/date data utilizing the output option that may be of lesser quality to ensure you have the information.

- On systems where the time/date stamp can be moved, ensure that this overlay does not obscure critical events.

- The amount of time and storage needed to retrieve the video data may dictate the best method for retrieval.

- Performing a test retrieval will assist in estimating the time and storage requirements for the chosen output option.

- Once the appropriate output option is chosen and the video data retrieved, a master should be retained. Depending upon the data retrieval method chosen, additional steps may be needed to create the master.

The following are all possible output options in their respective order of suggestion

The intent of "respective order" is to consider the list from beginning to end as being organized from most advisable to least advisable – from a technical and quality of service standpoint.

CD/DVD Writer

Many DCCTV systems have a built-in or external CD/DVD writer to retrieve the recorded video. In some instances, an external CD/DVD writer can also be connected through a USB/Firewire/SCSI port (see USB/Firewire/SCSI Devices).

- Generally, the DCCTV system software will have an archive, backup, copy, or export function in which you can retrieve the data directly to the CD/DVD writer.

- Generally, the system software will allow you to copy the proprietary viewer to the disc while burning, however, you may have to manually select this option.

- Write-once CD-Rs, DVD-Rs, or DVD+Rs should be used.

- Some drives may only write to a specific brand(s) of media. If difficulties are encountered when writing data, try another brand of media.

  Some DCCTV systems may only take a CD-RW/DVD-RW disc. If the data is downloaded to rewritable media, transfer the data to non-rewritable media or secure electronic storage as soon as possible. The transfer should be verified according to the methods outlined in SWGIT document "*Best Practices for Maintaining the Integrity of Digital Images and Digital Video*".

- The system may require you to format the CD/DVD, either in the DVR itself or in another computer.

- The system may require you to finalize the CD/DVD in the original recording device before the disc can be read in other devices.

- After retrieval, verify that the downloaded/exported file(s) play back correctly on another system, and that the proper dates and times were retrieved.

- If multiple files are retrieved, they should be named to ensure that the proper order of playback is identifiable.

- The resulting produced WORM media or file(s) on the secure electronic storage is the master evidence. If more than one disc is created, each should be identified for proper order of playback.

Flash Media

Some DCCTV systems have a flash card option, which is usually intended for short video sequences and should be used as a temporary storage medium only. Even though many cards now have the ability to hold gigabytes of information, the majority of these drives are not intended for permanent storage and are not as readily available as CD/DVD writers. If data is recovered via these drives, all data should be transferred from the flash media to a more permanent media to create the master evidence at the earliest possible time. The transfer should be verified according to the methods outlined in SWGIT document "*Best Practices for Maintaining the Integrity of Digital Images and Digital Video*". The drive should then be wiped before reusing.

Some systems require appropriately sized and formatted flash media (see the system manual for more information).

Some systems that employ flash media drives export files in real time (e.g., a 10-minute file will take 10 minutes to download/export). This may not be the most appropriate option for the retrieval of a large amount of data.

Mass Storage Devices

USB/Firewire/SCSI/eSATA ports can be used to connect external CD/DVD writers, drives, and legacy devices. It should first be established that the port is a working port. Some devices may require activation by installing the necessary drivers on the recording system. It is recommended that the manufacturer be contacted before attempting to install any drivers.

- External USB CD/DVD writers may be used for retrieving smaller amounts of data if no other option exists. External hard drives are a good resource when large amounts of data need to be collected.

- On some PC based systems that utilize a "standard" Windows operating system, it may be possible to copy the native/proprietary file(s) using Windows Explorer. **NOTE:** This does not work on all systems as the file(s) retrieved in this manner may require the use of the hardware/software during the retrieval process for playback later. It is strongly recommended to know the system before utilizing this method or to consult the manufacturer to ensure the file(s) copied will be capable of playback.

- Some DVR systems have a limitation on the amount of data that can be retrieved (downloaded/exported) at a time, typically 1 GB, sometimes 2GB. This limit may not

be specified in the system manual or known to the manufacturer. It is best to keep your file(s) under 1 GB, unless you know for sure it is capable of more.

- Generally, the DCCTV system software will have an archive, backup, copy, or export function in which you can retrieve the data directly to the device attached. You may have to choose the device or navigate to it.

- Generally, the system software will allow you to copy the proprietary viewer to the device, however, you may have to manually select this option.

- After retrieval, verify that the downloaded/exported file(s) play back correctly on another system, and that the proper dates and times were retrieved.

- If multiple files are retrieved, they should be named to ensure that the proper order of playback is identifiable.

- External hard drives are usually considered a temporary storage medium. Therefore, at the earliest possible time, all data should be transferred from the drive to a more permanent media to create the master evidence. The transfer should be verified according to the methods outlined in SWGIT document "*Best Practices for Maintaining the Integrity of Digital Images and Digital Video*". The drive should then be wiped before reusing. If the file(s) retrieved are too large, the external drive may be retained as the master evidence.

Network Connection

Many DCCTV recording systems have network ports. Furthermore, many DCCTV systems have their own proprietary network viewer software which allows for multi-computer connectivity and recovery of the native/proprietary recorded file(s).

If you do not have any experience with computers or networking, it is highly recommended that you obtain assistance prior to retrieving data using this method.

By utilizing an ethernet crossover cable, computer, and network viewer, a connection to the DVR can be established and the native/proprietary file(s) downloaded/exported. The remote or network viewer software is installed on a separate computer/laptop, the IP address of the DVR is usually configured in the remote viewer software, and a connection is established.

Verify that the network viewer recovers the native/proprietary recorded video file. **Example:** Some remote viewers only allow for the collection of still images and not the entire native/proprietary recorded video file.

- Ensure you have administrator rights on the computer/laptop to which you are downloading/exporting the file(s). Disable any firewalls.

- Screen savers should be disabled as they can interfere and/or disrupt the download/export process (See Appendix B).

- **Warning:** Power scheme settings for the computer to which you are downloading/exporting the file(s) should be set to 'always on' with hibernation disabled (See Appendix C-01 and C-02).

- The IP address may be required from the DVR. This usually requires accessing the menu functions of the DVR. Care should be taken not to change other settings on the DVR when doing this.

- Some proprietary remote/network viewers are installed on the DVR system for easy access. Otherwise, searching the vendor's website or contacting the vendor directly may be necessary.

- On some systems, setting up a standard Windows network connection between the computer/laptop and the DVR may be necessary (e.g., computer/laptop 192.168.10.1, and the DVR 192.168.10.2). **NOTE**: It is best practice to try and retain the existing IP settings on the DVR and change those on the computer/laptop to match.

- If a network viewer for the system does not exist, a connection may be possible utilizing Windows Explorer, a web browser, and typing in an appropriate IP address.

- If you have to change the IP address on the DVR, make note of the original IP address so you can change it back when you are finished. Changing the IP address may also require rebooting the system

- Some DVR systems have a limitation on the amount of data that can be retrieved (downloaded/exported) at a time, typically 1 GB, sometimes 2GB. This limit may not be specified in the system manual or known to the manufacturer. It is best to keep your files under 1 GB, unless you know for sure it is capable of more.

- Some networkable systems may only allow for the video to be "streamed" out and may not provide native/proprietary data transfer. Metadata can be lost through "streaming." Unless this is the only option, it is preferable to output to digital magnetic tape.

- Ensure network speed is sufficient to ensure that no possible data is lost and to prevent crashes/timeouts during downloading/exporting.

- You may have to disable any firewall, ensure you have administrator rights on the DVR. After completing data retrieval, confirm you have re-enabled the firewall and various settings.

- After retrieval, verify that the downloaded/exported file(s) play back correctly on another system, and that the proper dates and times were retrieved.

- If multiple files are retrieved, they should be named to ensure that the proper order of playback is identifiable.

- Ensure you have also retrieved the proprietary playback software.

- Return all changed system settings to their prior state after data has been retrieved.

- The computer/laptop or external hard drive(s) that you connected to the computer/laptop to retrieve the video file(s) usually are considered a temporary storage medium. Therefore, at the earliest possible time, all data should be transferred from the laptop or external drive to a more permanent media to create the master evidence. The transfer should be verified according to the methods outlined in SWGIT document "*Best Practices for Maintaining the Integrity of Digital Images and Digital Video*". If an external hard drive was used, then it should be wiped before reusing. If the file(s) retrieved are too large, the external drive may be retained as the master evidence.

Replacing Hard Drives

In some situations, the quickest solution may appear to be to remove the hard drive(s) from the system and replace them. This option should be considered carefully as there are many factors that come into play. Simply removing a hard drive(s) does not ensure the video contained on that hard drive(s) will playback. Some DVR systems require the actual DVR hardware to playback the video on the drive.

If you have limited computer hardware experience, consider calling someone for assistance. Care should be taken to follow appropriate health and safety procedures, particularly with regard to potential exposure to electricity.

- The system should be properly shut down prior to removing any hard drive, even if the drive appears to be "hot swappable."

- Ensure that all of the system's hard disc drives are retrieved. The system may have a removable drive in a caddy, but also additional internal drive(s).

- Document the master/slave drive configuration of all retrieved drive(s).

- The DVR may require a specific brand, model and size of hard drive to operate correctly. Consult the manufacturer, manufacturer's web site, or system manual for more information.

- The new drive(s) may need to be formatted by the DVR before it will recognize and record to it.

- Once the new drives are installed, restart the system and confirm that recording and playback are operational, as the system may require that vendor specific software/operating system be installed. Failure to install such software can render a system either partially or completely inoperable.

- If you remove the existing drive(s), be aware that you have removed the archive data stored on the CCTV system.

- The removed hard drive(s) is the master evidence. If more than one hard drive is removed, each should be properly identified.

Drive Duplication

In some situations, drive duplication may be necessary. This option should be considered carefully as there are many factors that come into play. Drive duplication does not ensure playback. Some DVR systems require the original hard drive(s) for playback.

It is recommended that a forensic clone of the original hard drive(s) be produced, not an image set.

- The system should be properly shut down prior to removing any hard drive, even if the drive appears to be "hot swappable."

- Some systems require the original hard drive(s) for proper operation. Therefore, if the drive(s) is duplicated, place the duplicated drive back in the system, make sure the system is operational, and retrieve the original drive(s) from the scene. If the system is not operational, the recording device may have to be retrieved, along with the original hard drive(s).

- Ensure you duplicate all the drives in the system as the DVR may have internal drives.

- Document the master/slave drive configuration of all duplicated drives.

- External playback software may exist to access the data on the duplicate hard drive.

- Upon initial inspection, a hard drive duplicated from a system may not appear to contain data when viewed using a standard PC. Many systems utilize proprietary formats that prevent data from being recognized. If you don't see files upon inspection of a forensic clone, the drive may still contain useful data.

- The forensic clone(s) and/or original drive(s) should be inspected using a write blocker and a separate computer/laptop.

- The forensic clone(s) and/or original drive(s) retrieved from the scene are considered the evidentiary master from which working copies may be produced.

Legacy Output

The following output methods usually enable retrieval of the native/proprietary video data and can be located inside the digital recording unit or as an attached external device. In some circumstances, this may be the only method available on the DVR system for retrieval of the video data. Retrieval and playback may require additional steps. These can typically be connected through the SCSI port. Do not discount this as a retrieval method if you do not have these devices.

- DDS TAPE (Digital Data Storage)
- Iomega Jaz
- Iomega Zip
- Floppy
- Magneto Optical

The above media should be considered a temporary medium. At the earliest possible time, all data should be transferred to a more permanent media to create the master evidence. The transfer should be verified according to the methods outlined in SWGIT document "*Best Practices for Maintaining the Integrity of Digital Images and Digital Video*".

Removal of DVR Unit

In circumstances where the above listed options have been rejected as either impractical or impossible, then the decision may be made to remove the recording unit itself.

This assumes that it is physically possible to do so, and that the removal is justified. For example, where the volume of data required is very large, it may be time efficient to temporarily remove the recorder and perform the retrieval in the lab, rather than on site. Alternatively, there may be no method for extracting the video data (e.g., CD writer or USB ports) and it may be necessary to remove the recorder and retain the unit as the evidentiary master.

- The recording device should be stopped and the system properly shut down prior to removal.

- Ensure all relevant components of the system are collected (e.g., power supply, remote control, dongle, manual, cables, hard drive keys).

- Ensure all cables are uniquely identified (e.g., camera inputs) to facilitate reinstallation of the system.

- If no other method exists for extracting the data from the DVR recording device retrieved from the scene, the DVR is considered the evidentiary master.

Non Native/Proprietary Data Retrieval

Although they record digitally, some DCCTV systems only have an analog output. For these systems, consideration should be given to collection of the DVR system as the master evidence. If this is not practical, then the following should be considered:

S-Video/Composite Output

- Video can only be retrieved in "real time" and the process should be repeated for each required camera view.

- When a system has both an s-video and composite output, it is recommended that the s-video be used.

- It is recommended that a digital video tape recorder (VTR) be utilized. Some examples of digital VTRs are Digital Betacam, DVC Pro, DVCam, Mini DV, and Digital 8.

- The video recording should be collected to digital magnetic tape.

- Ensure the "time/date stamp" is displayed on output; this may require checking several signals (e.g., composite and s-video).

- It is recommended that the DVR output be directly connected to the VTR and a separate output from the VTR be made to a monitor to ensure that the signal is being received and recorded.

- Prior to recording the video data, check and adjust playback speed on the DVR to "real time"or 1x.

- The collection of video data to VHS tape or Video DVD should be considered a last resort and conducted if it is the only possible option.

- Taking the analog output from a DVR may produce a different frame size from the original native/proprietary frame size.

- The produced magnetic tape is considered the evidentiary master.

NOTE: Video capture cards can be utilized for digitizing a video signal from the DVR to a computer. Most capture cards can take an s-video and composite input, while higher quality cards can input a component, SDI, and HD video signal. It is recommended that the highest quality signal be utilized. Care should be taken to ensure that the recorded frame size is maintained when utilizing this method. The digitized data should be captured as uncompressed (1:1) and retained as the master evidence.

VGA/DVI/HDMI Output

Some DCCTV systems have a VGA, DVI (DVI-A/DVI-I) or HDMI output that allows the video data to be displayed on a computer monitor. Devices are available that allow the DVI (DVI-D) and HDMI signals to be directly captured at their native resolution, while maintaining the signal's progressive scan format. Alternatively, a scan converter can convert a VGA or DVI signal to a standard video signal, usually analog, which can be recorded to video format and retained as the evidentiary master.

Either method should be considered a last resort as the final product may not include all metadata and image quality may be compromised. The latter is especially of concern with scan conversion as it can reduce image quality below that of an s-video/composite output.

Whenever possible, the footage should be captured at its native resolution (without scaling).

Important Information

- Do not change the time and date on the DVR system.

- It is not recommended that any additional software be installed on the DVR system (e.g., CD writing software, if it is not present). If it is absolutely necessary to install additional software, it is highly recommended that the manufacturer be contacted prior to installation.

- A DVR typically records data linearly. When the storage device is full, new data overwrites the oldest recorded data in a manner that is not recoverable. When data is deleted by other means (e.g. formatting the storage device), the space occupied by that data is marked as free for recording. Deleted data in this space may be recoverable for a limited amount of time before being overwritten. DVR file systems are typically non standard. Recovery of these file systems and the proprietary data is a difficult and time consuming process and may not be successful. Before seizing the DVR, check to see if the venue retains back up files and consult an individual trained in the interpretation and extraction of video data.

If it is determined that the video data of interest has been overwritten, check to see if the venue retains back up files.

- Administrative/Engineer access to the DVR usually allows more options for retrieval, including native/proprietary files.

- Time/date stamp with file. You may have to take the downloaded/exported file without the time/date data to ensure the highest quality footage, and take a second retrieval of the footage which includes the time/date data utilizing the output option that may be of lesser quality to ensure you have the information.

- On systems where the time/date stamp can be moved, ensure that this overlay does not obscure critical events.

- A review of the live monitor may appear to be of better quality than the actual recorded video.

- Whenever possible, the system should remain recording during the retrieval of the data.

- Many digital video recording systems allow you to auto-copy the proprietary playback viewer while retrieving the video data. This should always be done where offered. If the system does not allow this, steps should be taken to retrieve the correct version, with full functionality, required for playback/viewing.

- The native/proprietary video data should be retrieved. If time permits, and if the system exports a file that is in a non proprietary format (e.g., AVI) for quick viewing, consider collecting that as well as the native/proprietary.

- If the DVR has multi-camera capabilities, all the video data for the required area of interest should be taken as it was recorded. These cameras should be recorded in isolation, showing one camera full screen and not multi-cameras on a single screen (e.g., not 4, 8, and 16 on a single screen).

- Ensure that the frame rate upon retrieval is as near to recorded frame rate as possible.

- Ensure that the aspect ratio of the video data upon retrieval is as near to the recorded aspect ratio as possible.

- Working copies may be produced from the master evidence.

Evidence Handling Procedures

- To provide an audit trail, contemporaneous notes should be recorded detailing the course of actions taken.

- Initiate a chain of custody for the retrieved evidence, per agency policies.

- If transport of evidence is required, ensure the evidence is packaged and sealed appropriately based on the media (e.g., jewel cases for compact discs, anti-static bags and individual foam insert boxes for hard drives).

- Keep evidence away from magnets, excessive temperatures, and otherwise hostile environments.

Prior to Leaving Scene, Ensure That

- You have completed all the necessary documentation.

- You have collected all required video data.

- The retrieved video data plays back correctly, preferably on another system, and that the proper dates and times were retrieved.

- The proprietary playback software, network viewer, backup player, and/or archive software have been retrieved.

- The recording system has been returned to its original state (e.g., any changes to the system settings have been reset).

- The recording system has been verified as operational, preferably in the presence of venue personnel.

- If removing the recording system, ensure that all necessary peripherals have been retrieved.

- If you have retrieved the recording system, have legal implications been considered?

- Obtain contact information of venue owner, system installer and/or system manufacturer for future questions/reference.

Legal Issues

- Some DCCTV systems are used as both a DCCTV recording system as well as a business computer. This should be considered when it is necessary to remove the digital video recording system from the scene.

- Consideration should be given as to whether owner consent is necessary and applicable for removing the recording system.

- Ensure the scope of the search warrant encompasses the video data and necessary system components.

- Is it necessary or feasible to provide the business with a replacement recording device if their system has been removed?

- If you need to retrieve or replace the recording device's hard drive(s), will you be voiding an existing warranty on the system? If yes, have you received the proper level of authorization?

- If the DCCTV system is an instrumentality or fruit of the offense, seize it.

Recommended Equipment Needed

To enable retrieval from a variety of systems that will be encountered, a range of equipment is recommended. The following is a suggested list of equipment that should permit video data retrieval from the most commonly encountered systems:

- Laptop with:
  - CD/DVD writable drives
  - USB ports
  - Network port
  - Firewire ports
  - eSATA ports
  - Wireless access
  - Capability for installing proprietary viewers - ensure you are Administrator on this computer and there are no restrictions that would impede the download (e.g., firewalls, agency software)

- Flash media reader (multi-format)

- USB floppy drive

- Four port network switch/hub

- External CD/DVD writeable drive -- USB/SCSI/Firewire

- USB and Firewire storage devices in multiple sizes

- IDE, SCSI and SATA hard drives in multiple sizes (80, 160, 300 GB for backwards compatibility)

- Cables to include:

    - Network cables (crossover cable and straight patch cable)
    - Composite and s-video cables, as well as RCA to BNC adapters
    - Audio cables (RCA, stereo, and mono mini)
    - USB cables
    - Firewire cables (iLink, 400, 800)
    - VGA/DVI cables
    - Power cables
    - Extension cords

- Write blockers (IDE, Firewire)

- Blank Media (CD-R,DVD-R,DVD+R, DVD-Ram,CD-RW, DVD-RW, DVD+RW, Blu-ray)

- Blank flash media in varying sizes

- Video monitor (NTSC/PAL)

- Computer monitor

- Still camera with media

- Toolkit containing :

    - Flashlight
    - Anti-static strap
    - Mirror
    - Assorted screwdrivers
    - Pens
    - Permanent marker (appropriate for marking media)

- Digital Video Tape Recorder

- Analog Video Tape Recorder

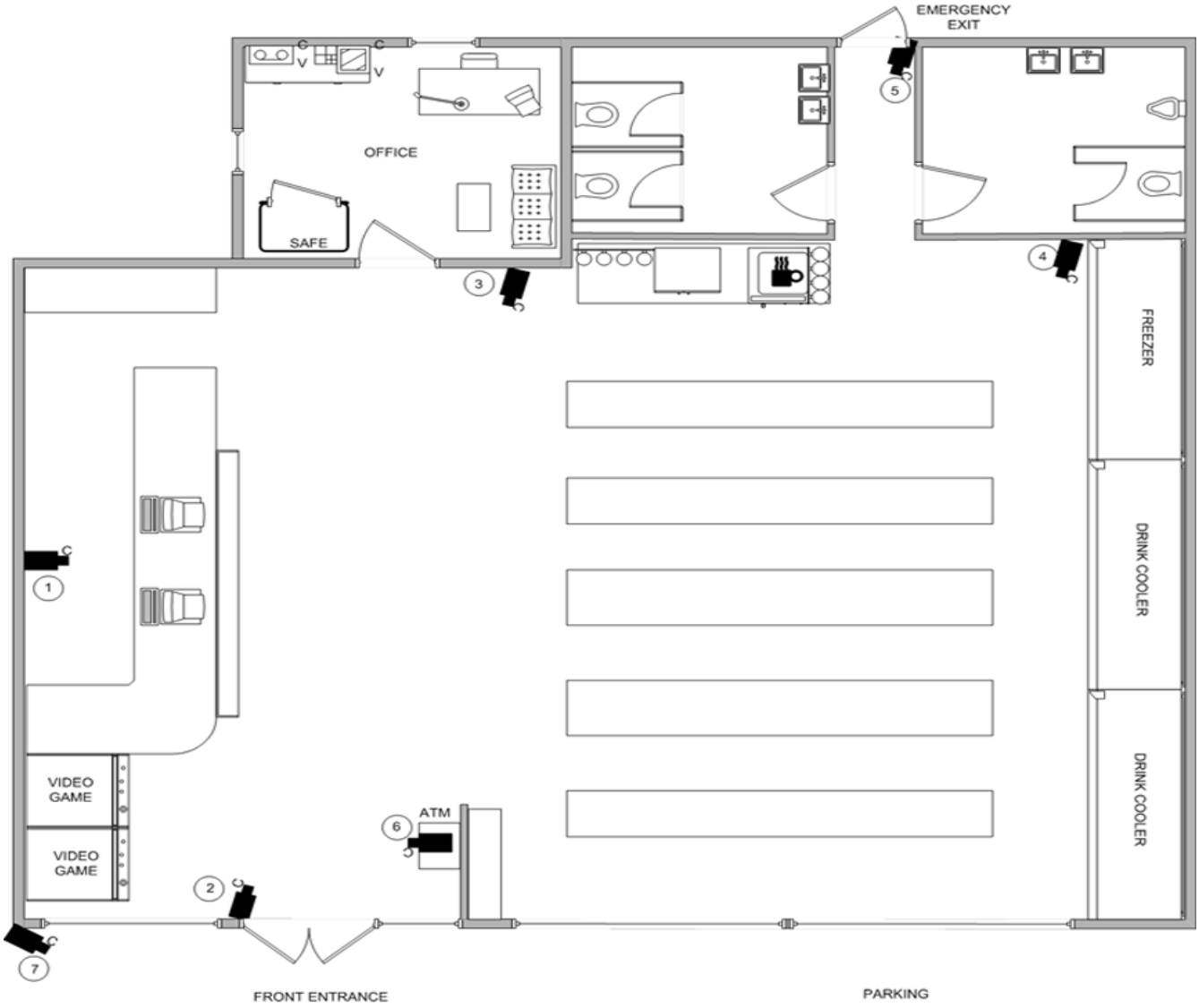
- Magnetic tapes (analog/digital)

- Appropriate forms (chain of custody, notes, consent)

- Appropriate evidence packaging (anti-static bags, jewel cases)

APPENDIX A

EXAMPLE OF SITE PLAN FOR
CONVENIENCE STORE

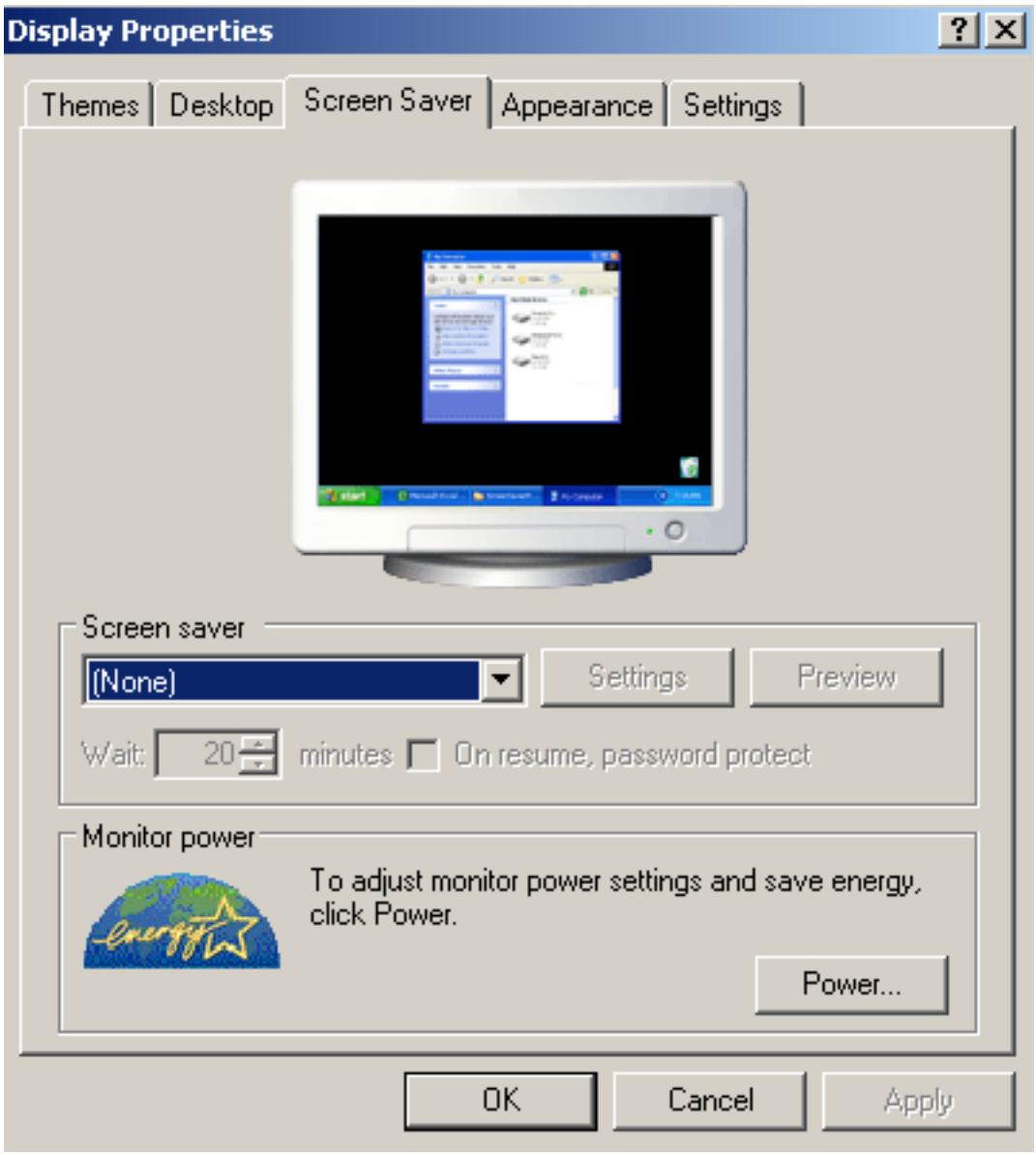


Camera 1: Clerk and check-out area, facing east
Camera 2: Front door entrance, facing north
Camera 3: Outside of office, facing south
Camera 4: Freezer area, facing south
Camera 5: Emergency exit, facing south
Camera 6: Automated teller machine, facing west
Camera 7: Parking lot, facing south-east

Taken from the Scientific Working Group on Imaging Technology (SWGIT) document, Section 4 "*Recommendations and Guidelines for Using Closed-Circuit Television Security Systems in Commercial Institutions*"

APPENDIX B

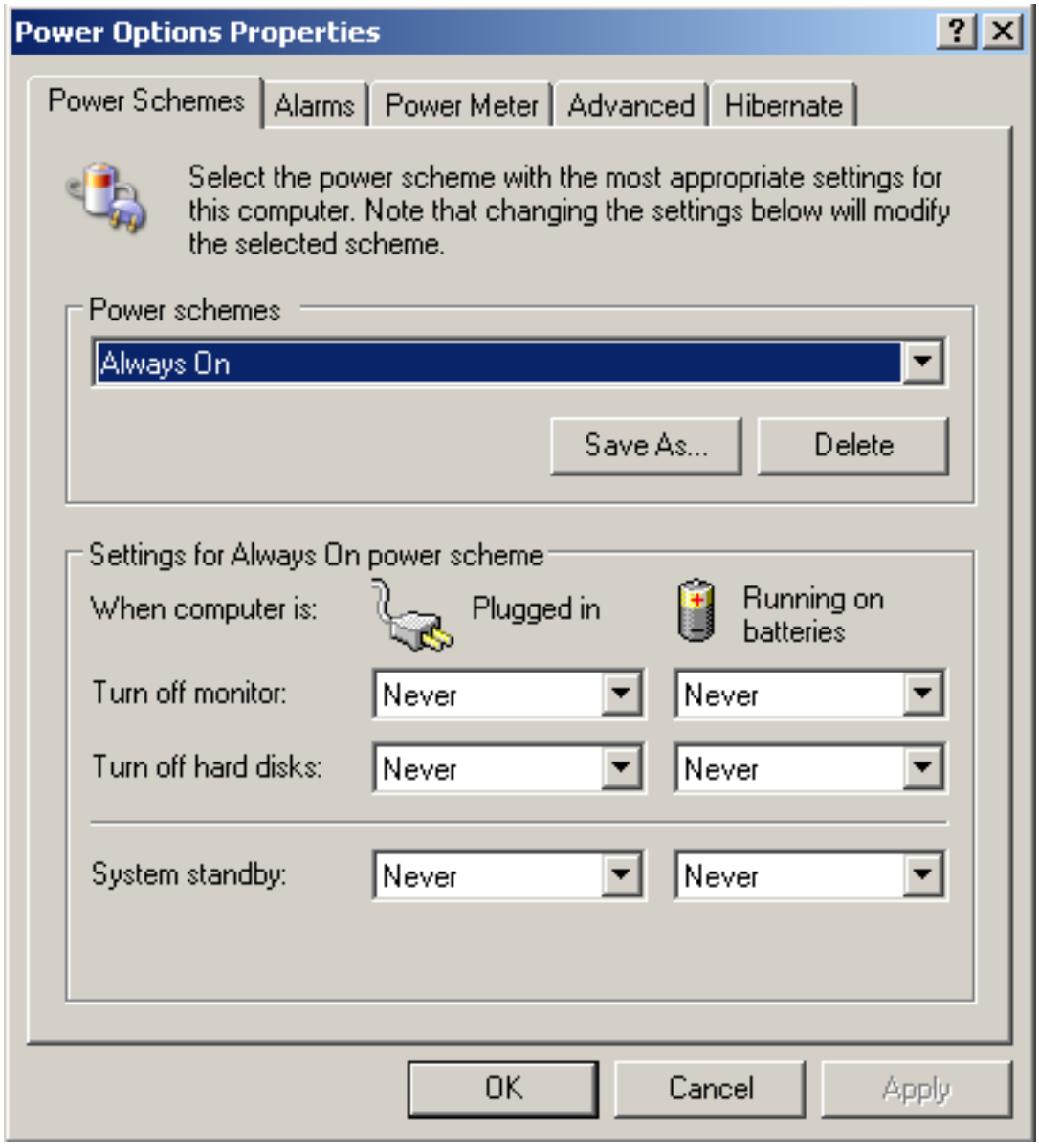
To access these options, refer to the system manual.



APPENDIX C-01

To access these options, refer to the system manual.

The following settings should be set as shown below.



APPENDIX C-02

To access these options, refer to the system manual.

Enable Hibernation should **NOT** be checked