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 15

Best Practices for Archiving Digital and Multimedia Evidence (DME) in the Criminal Justice System

INTRODUCTION

It is essential that agencies store their digital and multimedia evidence[1] (DME) in such a way and under conditions that will permit access when it is needed. Archiving is the process of storing data in a manner suitable for long-term availability and retrieval. The archiving process is more than just the preservation of physical media. In cases where archiving is desired, this should be planned for from the moment the DME is generated, processed or seized.

This document is intended to familiarize the reader with issues surrounding archiving DME and suggests best practices for establishing and maintaining an archiving program. This document is not intended to cover the archiving of administrative documents or public records but may prove useful in the archiving of non-evidentiary images, video, and related files.

Why Archiving is Needed

Archiving is needed to ensure that stored DME is available for future use. The techniques employed should be chosen to ensure that data can be located, accessed and used. DME is sometimes required to be stored for long periods of time per statutory requirement and/or departmental policies and regulations.

What Should be Archived

DME that you are legally permitted to possess and that may be required for future access should be archived. Keep in mind that it may be necessary to retain original software and hardware, or to transfer data from one type of media to another, in order to access archived DME in the future.

ARCHIVE CREATION

Archive SOP's

Departments should ensure that a written archive standard operating procedure exists and is implemented. (This SOP does *not* have to be a stand-alone document.) The SOP should take into consideration the department's long term goals, planning and needs. New technologies, court precedents and changing circumstances may dictate an SOP change. Previous versions of SOPs should be maintained as reference.

Physical Plant

Physical plant concerns are multi-faceted. One of the biggest issues is environmental factors that can have an adverse effect to the archive. Some of these factors include temperature and humidity control, electrical surge protection, fire suppression, natural disaster preparation and electro-magnetic field mitigation. The use of a secondary off-site storage facility is encouraged to provide a backup to the primary archive facility.

This document includes a cover page with the SWGIT disclaimer

Security

To ensure the integrity of the archive, security policies and procedures must be addressed by the agency. Security policies should address issues such as physical and electronic access tracking, limitation of access, virus detection and data suitability. In the event of an archive containing DME requiring a chain of custody, this issue should be addressed as part of agency policy and procedures.

Hardware / Software

As technology progresses, and hardware and software are upgraded or changed, it is possible the original hardware and software used to create/access the DME may need to be retained in functional condition to ensure accessibility. This is especially true in the case of proprietary systems.

Media

In the field of imaging technology, photographic plates, films, and photographic prints have been shown to be appropriate media for archiving purposes, provided they are developed and stored according to industry standards. Videotape has also demonstrated the ability to be stored for long periods of time without degradation when stored correctly. There are many types of media to which DME data can be written for the purposes of archiving. These include optical media (including CDs and DVDs), magnetic tape, and servers which may or may not include Redundant Arrays of Independent Disks (RAIDs). Serious consideration should be given to the type of media chosen for this purpose.

Many law enforcement agencies have chosen to use optical media as an interim solution for the storage of DME. Concerns about the actual versus theoretical lifespan of optical media have been raised. The lifespan of optical media begins at the time of manufacture, not at the time it is first placed into service. While optical media has been shown through common experience to be sufficient for short to moderate-term storage, it is inadequate for archiving. However, optical media used for any length of storage should be specifically designed for archival purposes and multiple copies should be maintained. Re-writable optical media should never be used for archiving as it has the shortest lifespan. Steps should be taken to ensure the serviceability of the optical media used by periodically testing and refreshing as required. (In the refreshment process, data from the original media is copied onto new media.) When media is refreshed multiple copies still need to be maintained. This process should continue until the DME is placed onto a different type of media, as technology advances, or the data is to be purged.

Some types of magnetic tape have been shown to be a reliable option in the long-term storage of data provided the media is refreshed as required per manufacturers' guidelines. At the time the archive is being planned and the use of magnetic tape archiving equipment has been determined, consideration should be given to the utilization of a magnetic tape format that is designed specifically for long term archiving purposes. Many of these devices make use of hardware and/or software compression in their storage of data. Compression concerns are addressed elsewhere in this document.

This document includes a cover page with the SWGIT disclaimer

RAIDs can be implemented using different configurations, which have varying levels of redundancy and fault tolerance. For example RAID Level 0 provides for no redundancy or fault tolerance, whereas other levels of RAID provide for excellent redundancy and fault tolerance. When RAIDs are used, agencies should determine their long-term needs and resources and choose the appropriate RAID configuration for their archives.

Media Preservation

The advantages and limitations of storage media, such as the unknown lifetime of optical disks, print fading, hard drive volatility and other manufacturer research data should be understood and incorporated into the archival structure. Utilize media recommended for long term storage when archiving data; in cases where servers are used, it may be necessary to have a backup solution. Media should be handled and stored in a manner consistent with the manufacturers' recommendations.

Data Transmission

When creating an archive consider the individual file size to be archived and the bandwidth available on the network in which the archive is established. Large or numerous files being transferred across a network may influence network performance. If the archive is not a dedicated system then the transfer rate of the network may be adversely affected.

Data Management

The integrity of the DME to be archived should be verified both before and after the creation of the archive[2]. Archived DME should be readily accessible via cataloging and indexing. The metadata[3] can be very useful for facilitating broad and accurate searches of the archive. Therefore, metadata should be archived with the data. Storage facilities should be adequate in size for the data to be maintained as well as allow for growth. (DME files can be very large in size and as technology increases file sizes will increase dramatically.)

Data Compression

Generally speaking there are two ways to approach the compression of data within the archive; hardware compression and software compression. When compression is used, it is imperative that the hardware and/or software used to decompress the data be archived.

Compression can be either lossless or lossy in nature[4]. Where practicable, it is recommended that data contained within the archives not be compressed. While lossy compression may not render an image unusable, such compression schemes are not recommended. (This is *not* to say that DME that was originally created in a compressed format cannot or should not be archived.) File type and content should be considered when determining the amount and degree of compression to be used.

When SOPs call for the conversion of proprietary formats to open source formats, it is advisable to use uncompressed formats when possible. If a compressed open source format is selected, lossless compression is highly recommended. As described above, less compression is best if the file must be compressed.

This document includes a cover page with the SWGIT disclaimer

Archive Maintenance

As new versions of hardware and software are released, backwards compatibility is not always ensured. Newer versions of software and hardware will not always be able to access the older data. It is necessary over time to ensure that the newer versions of software and hardware will be able to access the older data. Archivists should be aware that software providers occasionally cease support for their proprietary file formats. Long term retrieval capabilities require that *both* original hardware and software be archived.

Hardware and Media

Maintenance of physical devices and/or media may require preventative maintenance on a periodic basis per manufacturers and industry recommendations. This maintenance should be planned for at the time the archive is developed. Hardware and media should be periodically checked and/or tested for operability and serviceability. If it is found that the hardware or media is no longer serviceable, or obsolescence is foreseen, steps should be taken to migrate all data to a proven, stable storage solution as soon as possible. If failures are detected, the possibility of batch failures should be investigated.

Software

Because certain file formats or proprietary software may become unusable as technology progresses this software should be archived as necessary to ensure accessibility of DME created by the software.

Reverse Compatibility and Interoperability

Reverse compatibility is the ability of newer versions of software and/or firmware to access older file versions. Interoperability is the ability to access data across platforms or applications. These issues should be considered when upgrades to hardware and/or software are planned.

It should be noted that upgrades to the computer operating system may cause installed programs to operate erratically or not at all. When upgrading, it is recommended that the new operating system be tested on a similar type of computer system prior to implementation into the archive system. It is recommended that when the operating system is upgraded, previous versions be archived.

DATA MIGRATION

From time to time, it becomes necessary to move data from one type of media to another or to newer media of the same type.

Media Obsolescence and Lifespan

As technology progresses, media storage will evolve. Older versions of media may no longer be readable or supported and will become obsolete. To ensure uninterrupted archive capabilities, it may be necessary to migrate the DME to current media. Additionally, no media has been shown to be completely permanent. A schedule should be implemented to periodically re-write DME to new media based on industry standards and/or an understanding of the limitations of media.[5]

This document includes a cover page with the SWGIT disclaimer

File Formats

Proprietary formats are formats that are primarily supported by the company producing them. These formats may not be supported as new applications become available and as technology improves. When possible, DME should be retained in its original format *and* in a non-proprietary format. Additionally, the original accompanying proprietary software should be retained for future accessibility as addressed above.

ARCHIVE RETENTION PERIODS

Legal / Departmental Retention Requirements

The type of DME and its retention periods may be dependent upon statutory requirements and/or departmental policies. These may be different but the longer time will take precedence. Some mechanism should exist to identify this time period and should be included in departmental SOP.

Purging

Legal requirements, storage space issues and departmental policy may dictate a purge (complete destruction) of archived DME. The method(s) used should be adequate to ensure that the purge of the data and/or media is accomplished. Proper means of verification should be incorporated into the methodology and documentation of the purge and include the method(s) used and when it was accomplished.

DISCIPLINE SPECIFIC ISSUES

Some disciplines may have unique requirements or special circumstances related to archiving and should be considered at the time the archive is planned. File size, proprietary file types, specialized software, metadata, interoperability and bandwidth are all factors that need to be considered. Close collaboration between discipline subject matter experts, administrative personnel, and information technologists is required to insure appropriate archival methods are implemented.

ADDITIONAL REFERENCES

United States. National Archives. http://www.archives.gov/preservation/
(Includes: Storage and Conservation concerns and Technical Information)

United States. Library of Congress. Nov. 22, 2005: *Collections, Care and Conservation.* http://www.loc.gov/preserv/pubscare.html
(Includes: Photographs, Magnetic Media, Recorded Sound and Film)

United States. NIST. April 15, 2004. Information Technology: *Care and Handling of CDs and DVDs – A guide for librarians and archivists*. ISBN 1-932326-04-9. http://www.itl.nist.gov/div895/carefordisc/

This document includes a cover page with the SWGIT disclaimer

[1] Analog or digital media, including, but not limited to, film, tape, magnetic and optical media, and/or the information contained therein. *See SWGDE and SWGIT Digital & Multimedia Evidence Glossary*
[2] See SWGIT *Best Practices for Maintaining the Integrity of Digital Images and Digital Video*
[3] Metadata is information about the associated file or data. *See SWGDE and SWGIT Digital & Multimedia Evidence Glossary*
[4] Compression of a file is the process of making the file smaller in size. Some compression schemes result in the loss of data while others do not. *See SWGDE and SWGIT Digital & Multimedia Evidence Glossary*
[5] United States. NIST. April 15, 2004. Information Technology: *Care and Handling of CDs and DVDs – A guide for librarians and archivists*. ISBN 1-932326-04-9

This document includes a cover page with the SWGIT disclaimer