

Nevada Electronic Records Committee



Legal Requirements for Nevada's Public Electronic Records



Nevada State Library and Archives
2005



OFFICE OF THE GOVERNOR

KENNY C. GUINN
Governor

December 6, 2005

To All Departments:

Earlier this year, the Nevada Electronic Records Committee in concert with the State Records Committee approved a new version of the *Legal Requirements for Electronic Records*. This update was reviewed and approved by the deputy attorneys general for the Department of Cultural Affairs and the State Records Committee. This policy document is an excellent resource that should be made available to and used by all state government entities to ensure that the electronic records they create are legally admissible.

These guidelines provide an overview of the issues, highlight the applicable laws, and detail the best practice requirements that pertain to electronically based information generated by state agencies. Whether the record is an e-mail message, a word processing document, a spreadsheet, a scanned image, or a database, these records must be managed with the same diligence that is required for paper-based records.

A long-term view and careful planning can help overcome this risk and protect legal requirements for as long as the records must be retained. Therefore, agencies that are considering upgrading or adding electronic records systems or databases should carefully review these guidelines. Everyone in our agencies is in some way responsible for securing these types of records. Following the policies and procedures set forth in *Legal Requirements for Electronic Records* provides a way to help achieve this goal.

Sincerely,

A handwritten signature in blue ink that reads "Keith G. Munro".

KEITH G. MUNRO
Deputy Chief of Staff/General Counsel

KGM/lf

Legal Requirements for Electronic Records

Overview

Introduction Earlier this year, the Nevada State Library and Archives, the State Records Committee, and the Electronic Records Committee approved this new version of the *Legal Requirements for Electronic Records* for distribution statewide. We believe this policy is an excellent resource that should be made available to all state governmental entities who are considering the addition of a new electronic records system.

Nevada's governmental entities are relying more and more on electronic records. It is the responsibility of each entity to ensure that these records are authentic and trustworthy.

Authority NRS 378.255 Management and retention of records; recovery of records.

Audience This policy is for those who have direct and indirect responsibility for making sure that records are properly used and managed in their organization, to include, legal, IT, records custodians and officers, compliance officers, program managers, and records users.

Summary The policy covers the following areas:

1. *Admissibility and Rules of Evidence*. These rules are identified as an overview of the requirements of the courts and regulatory authorities to explain what makes a record trustworthy. Trustworthy records provide evidence of actual events; they must be complete, reliable and unchanging products of the activities that generated them.
2. *Evidentiary requirements for audits*. This section explains why the accuracy of records and the reliability of the systems that produced them come into question during the course of most audits.
3. *Measures to enhance the authenticity and legal acceptance of electronic records*. This section lists the practices and procedures that must be included in every electronic records system to ensure the trustworthiness of the records produced by the system.
4. *Special Considerations for Newer Technologies*. This section identifies components of new technologies:
 - *Originals versus Duplicates*: Discusses how the courts address electronic records stored on computer-readable media.
 - *Electronic Mail (E-Mail)*: Discusses the state policy on *Defining Information Transmitted via E-mail as a Public Record*. (**Appendix A of this document**)
 - *Digital Imaging*: Identifies precautions to ensure legal acceptance of digitally produced images.
 - *Electronic Image Format*: Identifies how to comply with the provisions of NAC 239.785.
 - *Electronic Signatures and Digital Signatures*: Discusses Electronic Signatures (NRS Chapter 720) and Digital Signature (NRS Chapter 179) technology.
 - *Electronic Data Interchange (EDI)*: Discusses electronic data interchange (EDI), the computer-to-computer exchange of business data.

- *Software Security – Copyright*: Discusses copyright laws.
- *Retention of Electronic Records*: Discusses records retention and media longevity.
- *Transferring Electronic Records to the State Archives*: Discuss records appraisal and records transferred to the State Archives.

For more information

If you need more information, please contact the State Records Management program at 775-684-3411 or records@clan.lib.nv.us.

To read more about legal compliance of electronic records, see *Information Nation: Seven Keys to Information Management Compliance* by Randolph A. Kahn, ESQ. and Barclay T. Blair, 2004, AIIM – available at the Nevada State Library and Archives.

**Sara Jones, Administrator
Nevada State Library and Archives
September 2005**

Legal Requirements for

Nevada's Public Electronic Records

Introduction

For more than three decades state and local governments throughout Nevada have used electronic technology to communicate, conduct business, provide information, and gain access to information. Electronic technologies have transformed the way state agencies create, use, disseminate, and store public records. As newer technologies are put into service, existing recordkeeping practices must be reviewed and modernized so that the records these new technologies produce are recognized as complete, reliable and trustworthy. Compliance with applicable legal codes, regulations, and agreements, with established applicable professional practices and standards, and with applicable administrative rules and policies is required.

This guide will discuss:

- ❖ Admissibility and rules of evidence
- ❖ Evidentiary requirements for audits
- ❖ Measures To Enhance The Authenticity And Legal Acceptance Of Electronic Records
- ❖ Special Considerations For Newer Technologies

THIS DOCUMENT IS NOT AN ATTEMPT TO GIVE LEGAL ADVICE.

If any questions should arise concerning any information given in this document, you are directed to seek the advice of your Deputy Attorney General or legal counsel.

ADMISSIBILITY AND RULES OF EVIDENCE

Courts admit records into evidence when the records meet specific criteria for admissibility. Admissibility refers to a court's willingness to accept records as evidence in legal proceedings. Modern rules of evidence – enacted into federal and Nevada state laws¹ – address two principle objections to the admissibility of records into evidence. First, the hearsay rule prohibits the admissibility of any out-of-court statements to prove the truth of a matter. Second, the best evidence rule precludes the admissibility of anything other than an original writing, barring an acceptable reason for the absence of the original. Neither rule is meant to preclude evidence that can be proven necessary and reliable, therefore, federal and state rules of evidence provide exceptions for overcoming the hearsay and best evidence objections. These exceptions contain the specific legal requirements for admitting records into evidence.

Since the Federal government and most states have adopted uniform laws with standard provisions for the legal admissibility of records, the rules of evidence for each will contain similar exceptions to the hearsay and best evidence rules. The following three uniform laws, drafted by the National Conference of Commissioners on Uniform State Laws, provide exceptions to the hearsay and best evidence objections in states that have enacted them. The most recent of the three, the Uniform Rules of Evidence, incorporates the provision of the two earlier rules and makes more explicit references to electronic records.

Uniform Business Records as Evidence Act (1936) establishes the admissibility of records created in the regular course of business if the sources of information, method, and time of preparation justify their admission. (NRS 51.135 and 51.145)

Uniform Photographic Copies of Business and Public Records as Evidence Act (1949) establishes the admissibility of duplicate records made in the regular course of business by any process which accurately reproduces them, provided the records are satisfactorily identified. (NRS 52.247)

Uniform Rules of Evidence (1974), modeled after the Federal Rules of Evidence, addresses the admissibility of both original and duplicate records. It incorporates the provisions in the uniform laws above, and addresses the admissibility of records produced or reproduced by modern information technology systems, defined as: "any process or system that employs a mechanical, photo-optical, magnetic, electronic, or other technological device for producing or reproducing records." (NRS 47 to 56 inclusive)

The rationale for the business records exception is that businesses depend on accurate recordkeeping to function effectively – records are generally considered trustworthy if created in the normal course of business. For example, records created to support typical business activities are more inherently reliable than records produced specifically for litigation. Creating records in the normal course of business is not limited to a pattern of activities that produces records on a cyclical schedule, i.e., daily, weekly, monthly – records also may be created at irregular times, such as ad hoc business reports.

For electronic records, NRS 51: "Hearsay" and NRS 52: "Documentary Evidence" are extremely important. Under the federal and state rules of evidence, original and duplicate records are admissible, provided the proper foundation is laid. Reproductions of original records must be produced in the regular course of business by a process that accurately reproduces the content of the records. Visible records, such as those produced with a computer in the form of computer printouts or computer output microfilm (COM), are considered originals if an appropriate witness can convince the court that they accurately reflect the information within the computer files². Generally, common information processing methods are more readily accepted as reliable than are newer information technologies, which may be subjected to greater scrutiny until their reliability can be established.

To fall within requirements of the rules of evidence, the record must be:

- Made by a public officer,
- In the form of a certificate or affidavit,
- Required or authorized by special provision of law,
- Made in the course of the officer's official duty,
- A record of a fact ascertained or an act performed by the officer,
- On file or on deposit in a public office of the state of Nevada.

Assuming that all of the above requirements can be met, the record will be considered *prima facie* evidence by a court of law in accordance with the provisions of the rules of evidence found in NRS 51.135, NRS 51.155, NRS 52.247, and NRS 52.260³.

Electronic Evidence for Administrative Hearings and Regulatory Proceedings

Nevada regulatory and oversight authorities have different procedural rules from courts. The rules of evidence for administrative hearings are contained in the Nevada Administrative Code (NAC) as established in accordance with the Administrative Procedures Act (NRS 233B). These regulations do not require agencies that hold administrative hearings to comply with the provisions of the rules of evidence, therefore, NAC gives agencies more discretion in determining what evidence will or will not be accepted in administrative proceedings. As rule-making bodies, regulatory agencies have the authority to enact formal regulations restricting the content and format of records that are acceptable for the hearings and regulatory proceedings they administer. These regulations may be more specific or more lenient than the rules of evidence that apply to admissibility in courts of law. Nonetheless, records must still be proven accurate and reliable. Because administrative decisions are generally subjected to judicial review, agency managers should use the provisions contained in the Nevada's Rules of Evidence to make sure that evidence used in administrative proceedings will also be acceptable if needed for a court challenge. Program managers should consult with legal counsel for advice on specific requirements that may be applicable to records needed for administrative hearings or regulatory proceedings.

EVIDENTIARY REQUIREMENTS FOR AUDITS

Accurate, reliable, and trustworthy records are the cornerstones of effective programs. Professional auditors should periodically perform audits to confirm that a system or process produces accurate results. Persons other than those who created the records or who have an interest in their content -- such as internal audit staff, Legislative Counsel Bureau (LCB) auditors, federal auditors, or independent auditing firms -- should perform the audits.

Typically, audits address financial and program issues rather than the accuracy of information systems, however, all audits utilize records that originate from information systems. Because auditors must concern themselves with the relevance, validity, and sufficiency of evidentiary matters, the accuracy of records and the reliability of the systems that produced the records may come into question during the course of the audit. With the ever-increasing complexity of government operations and with the introduction of new technologies, the accuracy of information systems has become a persistent audit concern that is no longer limited to the special area of data processing audits. Guidelines for legal acceptance of records are compatible with the evidentiary requirements for many audits. Program managers are also responsible for complying with any program, financial, or performance audit requirements that rely on creation and maintenance of accurate and trustworthy records.

MEASURES TO ENHANCE THE AUTHENTICITY AND LEGAL ACCEPTANCE OF ELECTRONIC RECORDS

The rules of evidence contain special provisions for establishing the authenticity and reliability of records. With the safeguards that can be built into today's modern information technology systems, the best evidence is not dependent on a specifically sanctioned technology used to create a record, but on showing that the record was the result of a process that accurately produced it (certification and documentation). When establishing the authenticity of electronic records, program managers must demonstrate in court or to administrative authorities the trustworthiness of the system used to produce the records. They, or a designated records custodian, may be required to testify about the operation of the system. In some cases, the opposing party or the court may be allowed to inspect a system.

When establishing the authenticity of records, agencies should focus on the reliability and accuracy of the system and process that produces the records, rather than on any innate characteristic of their format or medium. These attributes are established by:

- Written policies and procedures defining proper development, maintenance, and use of the system.
- Training and technical-support programs ensuring staff understand and correctly follow the policies and procedures.
- System controls monitoring the accuracy and authenticity of data, the reliability of hardware and software, and the integrity and security of the system.

Systems that produce records must produce the records in the normal course of agency business and in an accurate and timely manner⁴. To demonstrate that the system producing the records is reliable, the system's policies, procedures, training, technical-support, and system controls must be well documented. This documentation must be understandable, accurate, and accessible.

Although the general principles described in these guidelines are applicable to any recordkeeping system and to any type of storage medium, not all systems merit the same degree of monitoring and control. Development of effective systems and procedures to ensure legal acceptance of electronic records requires investments in systems analysis, procedure development, software, and training. Therefore, the stringency of controls should keep pace with the degree of risk and the benefits to be gained from more effective systems management. Governmental entities should focus on mission-critical systems – systems that produce records needed in legal proceedings and audits – and on systems that expose the agency to a high degree of risk. Systems that use newer technologies also warrant careful review because effective management practices for these technologies are still evolving.⁵

General Characteristics of a System or Process

Legal acceptance of electronic records requires proof⁶ that the process or system is reliable and therefore capable of producing trustworthy records. Records will be more readily accepted as trustworthy if an agency can demonstrate that the system can:

- produce the records as part of a business function.
- create accurate records.
- produce records in a timely manner or produce records after the fact (i.e., with a time lapse between an event and the creation of the record) that has no effect on its content.

Written Policies and Procedures

The policies and procedures define the normal operations of the information system's development, maintenance, and use. The trustworthiness of the records may be judged by the adequacy of its procedures and how well the procedures are followed. The policies and procedures must be kept up-to-date and should include:

- the methods used to create, modify, duplicate, and destroy records.
- the roles and responsibilities of the individuals involved in record creation, maintenance, and destruction.
- the quality control procedures, typical problem resolutions, and other activities that might otherwise subject the system to inconsistent action or misinterpretation.
- the purpose and uses of the system.

Established policies and procedures demonstrate the intent of any agency to manage and control the process or system. However, the trustworthiness of an agency's records also depends on if and how strictly the established policies and procedures are followed. Courts may scrutinize deviations from established procedures – especially if deviations are from legally required procedures. Therefore, additional measures are necessary to ensure that procedures are followed and deviations are detected and remedied.

Training and Technical Support

Formal training programs and technical-support programs help ensure that the staff understands and correctly follows the policies and procedures. Documentation, demonstrating that the agency provided sufficient supervision to oversee staff in the proper use and maintenance of a system, will strengthen the case that procedures were followed. Keep training records on attendance and certification. Keep technical-support logs and help-desk (trouble) reports, which document that problems were identified, attended to, and resolved. In general, if an agency can validate adequate staff instruction and supervision, they can demonstrate that procedures were likely followed.

Adequate System Controls

Effective recordkeeping systems, whether manual or automated, need mechanisms and controls to ensure the quality and reliability of the records produced. These controls monitor the input and output processes, hardware and software performances, and system security. Controls should be built into a system when it is developed

and embedded into its operating policies and procedures – then reinforced through ongoing training and support.⁷

System Audit Trails

Audit trails document who used the system, when it was accessed, what functions were performed, and the results of the use. Audit trails are either manual or automated. Manual audit trails normally follow a paper trail of sign-off sheets. An automated audit trail is generated by an internal auditing system that monitors internal system activity. Effective audit trails can detect who accessed system, what procedures were followed, and if any alleged fraud or unauthorized acts may have occurred. Automated audit trails track:

- any changes to data in a system, including the creation, modification, and deletion of records.
- the date and time of any changes.
- the source of any changes.

Information technology (IT) managers have an increasing variety of tools at their disposal for maintaining system audit trails -- such as keystroke monitoring, time and date stamping, virus detection, etc.

Routine System Performance Tests

Conduct regular, routine system-performance tests. Maintain operation logs and running schedules to document the reliability of system operation and performance. Systems rely on system edits and routine testing to verify the accuracy and reliability of the data -- the information collected will provide the necessary oversight to verify the integrity of a system and the reliability of the records it produces.

Hardware and Software Reliability

Malfunctioning equipment and/or computer programs can challenge the reliability of the system and erroneously alter the content of computer records produced by the system. To enhance the acceptance of the system-generated records and to document the reliability of system performance, system managers should:

- routinely test the hardware and software performance, per manufacturer/developer recommendations.
- retain all documentation related to hardware and software procurement, installation, and maintenance.
- maintain and retain operating logs and run schedules.

Security

Secure systems furnish an ideal environment for creating and maintaining trustworthy records. To achieve a secure system, developers must build in routines that will prevent unauthorized modification of data. These routines must be documented to backup the credibility and trustworthiness of the system.⁸

- Divide the duties of staff so that individuals with an interest in the contents of records are not responsible for administering system security, quality control, audit, or other tasks where the integrity of a system can be compromised or called into question.
- Develop and test disaster preparedness plans and security back-up procedures to ensure that records are protected against inadvertent or accidental loss or destruction.
- Document any back-up procedures used to restore a system or recover records, especially if these procedures were used to generate a record.

Controls for Accuracy and Timeliness of Input and Output

The processes used for data input and output must produce accurate and timely records. Input can be challenged on any of the following grounds:

- The manner in which data were entered into the system initially.
- Whether the data were entered in the regular course of operations.
- Whether data were entered within a reasonable time after the events recorded.
- The adequacy of measures taken to ensure accuracy of the data.

The acceptance of records generated through processes that involve input and output, by taking the following measures:

- Develop and follow systematic procedures for data entry.
- Design, implement, and document the quality control procedures.
- Identify all input and output documents and procedures in the system documentation.
- Attest to the accuracy and validity of records at the time they are created or updated.
- Document any delays in data entry by keeping records of the date the original source documents were created and the date the data were entered. Keep records of any unusual delays in output.
- Retain any specially written program used to extract data from a system.
- Produce labels for off-line media (e.g., CD's, DVD's, tapes, diskettes, etc.) containing electronic records that identifies the exact title, creating program (and operating system), date, purpose, source, and destination of records.

These measures will enhance the accuracy and reliability of records for legal admissibility and other purposes.

Comprehensive System Documentation

An essential ingredient for demonstrating the trustworthiness of the records is the documentation of the system or processes that produce the records. This documentation authenticates the processes that produce the records. Documentation should include all aspects of the system's design, implementation, maintenance, and oversight, and if applicable, the migration and/or conversion procedures that were followed. The documentation should be systematically updated – if an older system was implemented without it, create the documentation as soon as possible.

Development guidelines: the documentation should be:

- comprehensive, covering all components of an information system, and demonstrating all steps from the beginning to the end of the process;
- prepared and maintained by knowledgeable staff; and
- clear and concise so that both current and future employees will be able to testify on its reliability.

Documentation can be introduced into evidence: for example, courts may request documentation that shows how the system operates, what training was conducted, what audit-trails are available, or any other records that may demonstrate if proper procedures were followed.

Documentation Retention

System documentation must be retained for 6 years after the system is decommissioned. As a system is modified or upgraded, preserve the older versions of the documentation for the complete lifespan of the system. Destruction, deletion, or other disposal of the documentation must be in accordance with agency retention and disposition schedules. The General Records Retention and Disposition Schedules, maintained by the Nevada State Library and Archives' (NSLA) Records Management Program and approved by the State Records Committee, identifies the retention and disposition of common types of hardware, software, system, and data documentation⁹.

SPECIAL CONSIDERATIONS FOR NEWER TECHNOLOGIES

Courts readily accept records produced by familiar information-processing methods and technologies, such as writing, typing, photocopying and microfilming. In fact, many of the policies and guidelines that permit use of reproductions of records are based on decades of experience with micrographics and established standards for quality reproduction. Records produced with newer technologies may be subjected to greater scrutiny because standards and practices for these technologies are not as well established.

Originals versus Duplicates

Rules of evidence generally have no bias toward originals, duplicates, or any particular technology – provided that proper procedures are followed and safeguards are in place to produce reliable, trustworthy records. Before a court an "original" of a record is the "*record itself, or any counterpart intended to have the same effect*" (NRS 52.205). In the case of electronic records stored on computer-readable media, a strict interpretation of the term "original" is impractical because a computer record cannot be viewed or read unless it is printed or displayed in human-readable form. To address this problem, most courts consider computer printouts and other eye-readable renderings of computer records to be originals, provided that they accurately reflect the information in the original recording. When records are captured by scanning and stored as digital images, the digital image or a printout of the image may serve as the best evidence in lieu of the original, if the records are adequately identified and accurately reproduced.

A "duplicate" is defined in the Nevada Rules of Evidence as "*a counterpart produced by the same impression as the original, . . . by mechanical or electronic re-recording, . . . or by other equivalent techniques which accurately reproduce the original*" (NRS 52.195). Duplicate records must be accurate reproductions of the original records – information readable or recognizable on originals also must be readable and recognizable on duplicates. Some images may have data files that store production, control, indexing, certification or other data on the image. This allows additional data (i.e., metadata) to be included but does not adversely affect the accurate reproduction of the record.

Imaging systems should not be capable of altering a record as scanned, except for standard image-enhancement routines used to improve legibility. If image enhancement techniques (i.e., techniques for processing the image so that the result is visually clearer than the original image) are used, the information that is readable or recognizable on duplicates must also be readable or recognizable on originals. In some cases, it may be necessary to document how the changes were made. It may also be advisable, once an image is captured and prior to any image enhancement, to store an un-altered reference copy.

Electronic Mail (E-Mail)

In 2003, the State Records Committee, as part of its legislatively mandated authority over the retention and disposition of records (NRS 239.073 *et seq.*), adopted a formal State E-mail Policy.¹⁰ The Administrator of the NSLA, and in accordance with NRS 378.255, adopted the policy as an official state standard. [Appendix A: Policy on Defining Information Transmitted via E-mail as a Public Record.](#)

Digital Imaging

Digital imaging uses scanning technology to capture and convert documents to a digitized format. Digital images are stored on magnetic or optical media and are displayed on computer screens or reproduced on paper. Because imaging is a relatively new technology with new potential for image enhancement and alteration, special precautions should be taken to ensure legal acceptance of digitally produced images.

Governmental entities using digital imaging technology should refer to the State's Electronic Records Guidelines, approved May 2000.¹¹ The following measures, as part of the normal operation of an imaging system, should be implemented:

- Verify that the system accurately reproduces all originals -- information that is readable and recognizable in the original is recognized on the digital image. Many imaging software applications include utilities to automatically verify the accuracy of the image when captured. If automated verification is not available, then visual verification of each image is necessary. The methods used for image verification should be described in the documentation of the system's operating procedures.
- Use the standard compression and decompression algorithms, as established by the Consultative Committee on International Telegraphy and Telephony (CCITT), to ensure long-term availability of the image in its original form. Proprietary algorithms do not guarantee the same degree of long-term readability and trustworthiness.
- If image enhancements are used to increase the legibility of documents in imaging applications, preserve a record in its "originally captured form" in standard compression and decompression algorithms, as established by the Consultative Committee on International Telegraphy and Telephony (CCITT). CPLR 4539 permits use of an enlargement or facsimile as long as the original is also available for inspection. The application of this requirement to enhanced digital images has not been tested in court. Any use of image enhancement must be part of normal operating procedures that are thoroughly described in the system's documentation.

- Institute security provisions that will prevent any alteration of digital images. Limit system access and update privileges to appropriate persons and prevent unauthorized modification of imaged records. Use system security features, such as password-controlled access, operation logs, and audit trails, to prevent any unauthorized deletions or modifications. Record who used the system, what they did during use, and the results of the use. Stress the importance of segregation of duties between system users and system operators.
- For off-line storage, only non-rewritable storage media is acceptable. Choose media that is a non-erasable and cannot be modified after the initial recording. ROM (read-only memory) disks store images that cannot be removed or edited by the user. CD-ROM and DVD-ROM are the most common types of ROM disk. Some CD-ROM and DVD-ROM have engraved serial numbers as well, which eliminates the possibility that altered disks might be substituted for originals. WORM (write once, read many) disks are also known as read-write optical disks. The most common form of WORM disk is CD-R (recordable). There is no single standard for WORM disks, which means they are typically only readable by the drive on which they were written.

Electronic Image Format: the Legal Requirement

In order to comply with the provisions of NAC 239.785, all imaged records, in their final form, must be placed onto a non-proprietary TIFF¹² format. This legal obligation allows for the image to be viewed in a universally accepted image format. Compliance will help to mitigate compatibility problems between systems. Conversion of documents to TIFF image formats will also help to reduce the potential that a document stored on a document management system could be altered without version and audit controls.

New versions of documents should always be stored as new TIFF Images. Older versions of a document must not be deleted without the legal authority to do so and all versions of a document should be cross-referenced.

Electronic Signatures and Digital Signatures

Governmental entities requiring Electronic Signatures (NRS 720) or Digital Signature (NRS 179) technology are advised to seek legal counsel and require the participation and expertise of four additional disciplines:

- Records managers.
- Security consultants.
- Technology consultants.
- Governmental entity subject matter experts.

Understanding the laws and technologies involved to ensure that an electronic document is properly authenticated is not for the faint of heart. Caution is the word of the day when implementing electronic signatures.

Contact the Nevada's Attorney General's office, the NSLA state records manager, and the Department of Information Technology for guidance regarding the use of electronic signatures for authentication of electronic documents.

Also, refer to "Records Management Guidance for Agencies Implementing Electronic Signature Technologies" published¹³ by National Archives and Records Administration (NARA) for guidance and as an overview of the issues.

Electronic Data Interchange (EDI)

Electronic Data Interchange (EDI) is the computer-to-computer exchange of business data. Most EDI applications include special measures to ensure authenticity as a substitute for the signatures on paper documents that have been used traditionally to authorize business transactions. In order for EDI to work as an effective and reliable method of transacting business, the trading partners involved must reach agreement on a number of technical and use standards that affect the meaning and validity of the data exchanged. Technical issues include provisions for the structure and format of data into transactions sets (also called "documents"), the transmission of formatted data, the standards for communications, and security procedures. Trading partners must also agree on what transactions sets will be exchanged, the meaning of data elements in those transactions sets, and instructions for how they are to be used. Issues related to contract formation, validity, and enforceability have to be addressed specifically within the context of each EDI relationship. For example, the time and manner in which electronically transmitted messages become effective, what constitutes an

electronic "signature," and the proper course of action in the event of an unintelligible transmission need to be established in contracts or memoranda of understanding among the trading partners.

The American Bar Association has developed Model EDI Trading Partner Agreements that provide a framework for the parties to reach agreement on these issues and confirm their mutual intent to give legal significance to EDI transactions. In the private sector, the need for standard formats and the fact that many of the issues relate to the business practices of specific industries has led to a growing number of very specific EDI standards for particular types of business transactions. In the public sector, governments are developing standards for common types of EDI transactions. Program managers are advised to consult their agency's counsel on the full range of legal issues involved with the use of EDI.

Software Security - Copyright

Federal copyright law protects software from the moment it is "*fixed in a tangible medium*". The rights granted to the owner of a copyright are clearly stated in the Copyright Act, which is found at Title 17 of the United States Code (17 U.S.C. § 102 *et seq.*). The Act gives the owner of the copyright "*the exclusive rights*" to "*reproduce the copyrighted work*" and "*to distribute copies ... of the copyrighted work*" (Section 106). It also states that "*anyone who violates any of the exclusive rights of the copyright owner ... is an infringer of the copyright*" (17 U.S.C. § 501), and sets forth several penalties for such conduct. Persons who purchase a copy of software have no right to make additional copies without the permission of the copyright owner, except for the rights to (i) copy the software onto a single computer and to (ii) make "*another copy for archival purposes only*," which are specifically provided in the Copyright Act (17 U.S.C. § 117).

Retention of Electronic Records

In accordance with NRS 239.080 to NRS 239.125, executive-branch agencies must have an approved records retention and disposition schedule that has been developed by the NSLA and approved by the State Records Committee prior to destruction of any official state records. Local governments cannot dispose of any public record except in accordance with a schedule for the retention of such records that is approved by the State Archivist (NAC 239.155). This includes source documents for automated systems and documents that are converted to digital images. The approved records schedule gives the agency and local government the legal authority to destroy obsolete records and establishes a plan for the orderly and normal-course-of-business disposition of records. Several factors are considered when determining whether to authorize destruction of source documents that are stored electronically or original records that have been converted to digital images (NRS 239.080; NRS 378.255 to 280; NAC 239).

By following the guidelines in this booklet, governmental entities increase the likelihood that records produced with today's technology will be legally acceptable. However, guaranteeing ongoing access to electronic records involves ensuring continuous readability for the life of the records. In an era of rapidly changing technology, access to long-term records¹⁴ may be difficult to ensure. Such factors as hardware/software obsolescence, media longevity, and records retention periods must be considered when determining if digital retention is sufficient, or if an alternative backup, such as paper or microfilm, must be established to meet minimum retention requirements of long-term records. All decisions about retention of original and digital records should be made in consultation with the Records Management program staff, 775-684-3411.

Transferring Electronic Records to the State Archives

The State Archives maintains the state's historically valuable records (NRS 378.230 *et seq.*, SAM Sections 2002.0 to 2052.0). Agencies transferring electronic records to the State Archives must first have them appraised for historical value and then certify them in accordance with NRS 52.260. Records that are accepted into the State Archives are in the legal custody of the State Archives and not of the agency that transferred them -- except as provided by law (NRS 378.250, NRS 378.260, and NRS 378.320).

If an agency's records retention and disposition schedule states that a records series is to be transferred to the State Archives, the agency's records officer should:

1. Contact the State Archives staff for the transfer of records.
2. Provide a typed inventory of the contents of the files (by file heading) and specify the medium to be used for transfer.
3. Transfer records on-line at a scheduled time.
4. Make special arrangements for voluminous material or electronic records with specific security concerns.
5. Provide hard copy of the system documentation (as appropriate) as requested by the State Archives.

6. Send a letter of transfer with records, so there is documentation of the transfer to the division.

If an agency does not have a records retention and disposition schedule but thinks they may be holding records of historical value, the agency should ask the State Archives staff to appraise the records. If the records are determined to be of historical value, the State Archives can receive these records under NRS 378.250.

Appendix A

STATE OF NEVADA

Policy on Defining Information Transmitted via E-mail as a Public Record

Introduction

Electronic mail or "E-mail" is a tool used to transit information between two or more parties. Information sent or received via e-mail is in many ways identical to regular postal mail that must be sorted and managed.

The State Records Management Program studied the e-mail policies of 26 other states. The findings demonstrate that many states continue to struggle with how to classify information received via e-mail as public record or non-record categories. This document provides guidelines on how to classify information contained within e-mail transmissions and defines a State of Nevada Policy for dealing with information contained within e-mail when it is classified as public record.

It is important to note that the information contained within an e-mail should not automatically be defined as a public record. While the content of some e-mail transmissions may constitute public records, others are simply personal mail, duplicates, transitory items, and other types of non-record transmittals that can be acted upon and quickly deleted. It is important to understand the distinction between public records (i.e., official state records)¹ and non-records² and the requirements of each. It is also important to understand that defining an e-mail as a public record is independent of the question of whether the record is confidential³.

This policy shall apply to all State of Nevada employees, as well as all individuals contracted to perform work for the State. This policy is to be used in conjunction with the Department of Information Technology (DoIT) Standard 5.6 Internet/Electronic Mail.

Types of E-Mail Transmittals & Appropriate Disposition

The State Records Program classifies information contained within e-mail transmissions into four basic categories:

1. Personal Messages
2. Transitory Messages
3. Duplicate Records
4. Public Records

Every public employee who uses e-mail to transmit or receive information in the course of conducting State business must be trained and knowledgeable on his/her responsibilities for managing public records. The difficulty in this responsibility lies in determining which e-mail message contains information that constitutes a public record. This issue is further complicated as the classification of a message as a public record may differ between the sender and the receiver(s), since it depends on the affect the information has on the business operations of the party who may subsequently receive the information.

All information sent via e-mail should be prepared under the assumption that:

1. Information sent via e-mail is not confidential.

2. The targeted recipient may not be the final recipient.
3. The information sent may be determined to be and maintained as a public record by another party.

As such, public employees should prepare all e-mail transmittals to be a professional representation of the agency for which they work. This includes, but is not limited to, the appropriate level of formality for the targeted and possible recipient(s), correct spelling, grammar, and punctuation, and use of appropriate labels, titles, salutations, and closings.

Additional standards under the authority of the Department of Information Technology (DoIT) regarding use of the State e-mail system may be found at:

1. <http://psp.state.nv.us/>
2. <http://gitoc.nv.gov>

State employees should be trained in classifying information contained within e-mails into one of the following categories. Once properly classified, the information contained within the e-mail may be processed per the recommended disposition.

Personal Messages: E-mail has evolved into a substitution for the telephone and is a cost-effective means of communication that is often used by State employees for communication that has no bearing or relevance to conducting State business (i.e. "let's do lunch" or "can I catch a ride home" types of messages). State employees should be aware that there is no guarantee of privacy or confidentiality for personal messages transmitted via the e-mail system as all messages are owned by the State and their contents may be monitored, viewed, printed, and further distributed at any time by other State employees.

NRS 281.481(7) provides State agency discretion to allow limited use of time, governmental property, equipment or other facility for personal purposes if: 1) the use is authorized by the appointing authority; 2) the use does not interfere with the performance of the employee's public duties; 3) the cost or value related to the use is nominal; and 4) the use does not create the appearance of impropriety. This is not to suggest that an appointing authority may not establish policies preventing the use of e-mail for personal purposes. However, the appointing authority should consider the realistic ability to police any such policy as well as ensuring consistency in any action to be taken for violations of any such policy (i.e., action cannot be taken against a single employee caught sending or receiving a personal e-mail if other staff are also known to be sending and/or receiving personal e-mails).

Disposition: Personal messages are not public records and may be deleted immediately after receipt.

Transitory Messages: These types of messages do not set policy, establish guidelines or procedures, document agency business, certify a transaction, or become a receipt. The informal tone of transitory messages might be compared to communication during a telephone conversation or conversation in an office hallway. These messages tend to convey information of temporary importance in lieu of oral communication and have a very limited administrative value. Many of these may have an official context, but may not be part of a business transaction. Examples of messages that are not public records include general departmental correspondence regarding routine business activities (transmittal messages and responses to routine questions); minor non-policy announcements; interoffice messages regarding employee activities (holiday parties, etc.); phone calls; published reference materials; invitations and responses to work-related events (meetings, etc.); listserv messages other than those posted in an official capacity (unless the messages are relied upon in the development of management, financial, operating procedures, or policy matters).

Disposition: Transitory messages are considered non-records and may be deleted may be deleted when no longer administrative useful, i.e., when the message has no value to the agency.

Duplicate Records: E-mail as a medium promotes expedited communication to multiple users with great ease. Consequently, e-mail systems frequently contain duplicates of a record, such as copies or extracts of documents distributed for convenience or reference. "All Agency Memorandums" are often forwarded via e-mail within the State system in order to speed up distribution of certain critical and/or time-sensitive information. Information transmitted in this manner is simply a duplicate or non-record. The paper document received in the State mail system is the actual public record.

Disposition: Duplicate records are not public records and may be deleted immediately.

Public Records: Public records are information and other documents created or assimilated in the course of conducting public business that document the activities and business of public employees. An official State record includes "any materials which are made or received by a State agency and preserved by that agency or its successor as evidence of the organization, operation, policy or any other activity of that agency or because of the information contained in the material" (NRS 239.080(4)(d)). If there is any doubt, a State employee should assume the information is a public record. Examples of information that could be transmitted in an e-mail that may constitute a public record include:

- Policies and directives
- Correspondence or memoranda related to official business (excluding duplicates)
- Work schedules and assignments
- Agendas and minutes of meetings
- Drafts of documents circulated for comment or approval
- Any document that initiates, authorizes, or completes a business transaction
- Final reports or recommendations

Once an e-mail transmittal is determined to be a public record, public employees of the State of Nevada have an obligation to apply the appropriate records retention schedule. For retention purposes, the records should be maintained in an easily accessible location, which may include:

1. Printing out a copy and filing a hard-copy in the relevant subject matter file, or
2. Moving the file out of the e-mail system and storing a copy of the e-mail in an electronic document management system.

Disposition: Public records should be retained for the period appropriate to their content and handled in accordance with approved records disposition authorizations (RDAs) (NRS 239.080).

Just as with any information maintained in an electronic format, agencies considering maintaining e-mail transmittals determined to be public records in an electronic format face unique challenges that must be addressed as agencies develop policies to meet the records retention requirements. Agencies contemplating maintenance of public records in an electronic format (as with any electronic record) must establish policies and procedures, taking the following minimum requirements into consideration:

- Establishment of a repository for holding and managing electronic files
- Policies which ensure that metadata information contained within the e-mail transmission is included in the public record (headers, forward headers, and transmission data)
- Procedures which address the ability to efficiently locate specific files when necessary
- Policies and procedures that ensure records remain fully accessible throughout the entire records retention period, including hardware, software, and data migration plans for electronic records that must be retained for six (6) years or more

Note: When there is doubt about the retrievability of an electronic record over its life span, the record should be printed and maintained in a hard copy format.

Permanent public records are archival records with legal, administrative or historical value that must be retained indefinitely. These records must be preserved in a medium that can be used by future generations. Since no medium used to store electronic records is considered permanent, public records for permanent record storage cannot be maintained in an electronic medium. Records appraised as permanent must be converted to paper, microfilm, or another acceptable medium for permanent records retention (NAC 239.760(3)(5)). If or when an electronic medium is judged permanent, this policy will be re-evaluated and appropriate changes made.

Notes to E-Mail Policy

¹ **NRS 239.080(4)** - Papers, unpublished books, maps and photographs; information stored on magnetic tape or computer, laser or optical disc; materials which are capable of being read by a machine, including microforms and audio and visual materials; and materials which are made or received by a state agency and preserved by that agency or its successor as evidence of the organization, operation, policy or any other activity of that agency or because of the information contained in the material.

² **NAC 239.705** -...published books and pamphlets, books and pamphlets printed by a governmental printer, worksheets used to collect or compile data after it has been included in a record, answer pads for a telephone or other informal notes, ...unused forms except ballots, brochures, newsletters, magazines, newspapers ..., scrapbooks, and property left or deposited with an office or department which would otherwise be defined as a record except that the ownership of that property does not reside with a local governmental entity.

³ **NRS 239.010 (1)** - All public books and public records of a governmental entity, the contents of which are not otherwise declared by law to be confidential, must be open at all times during office hours to inspection by any person, and may be fully copied or an abstract or memorandum may be prepared from those public books and public records...

Acknowledgements

Excerpts from *State Government Records Management Information Series: Guidelines for the Legal Acceptance of Public Records in an Emerging Environment* (Albany, New York: University of the State of New York, State Education Department, 1994)

John Paul Deley, Electronic Records Archivist and Robert H. van Straten, State Records Manager, of the Nevada State Library and Archives, first produced this work, which was approved by NERC on October 17, 2001.

NERC, chaired by Teri J. Mark, CRM, State Records Manager, began the process of revising it in October of 2003. The workgroup assigned this task was directed by Thomas Allsteadt, Information Systems Coordinator of the City of Las Vegas and staffed by Robert H. van Straten, now Senior Records Analyst. The NERC Steering Committee approved the revision on November 9, 2004, at which time it was forwarded to the State Records Committee for final approval. The State Records Committee approved it on January 12, 2005. Deputy Attorney General James E. Irvin reviewed the legal citations for accuracy and completeness. State Archives Manager Jeffrey M. Kintop formatted this publication and designed the cover.

The Nevada State Library and Archives, a Division of the Department of Cultural Affairs, assisted with this document and has acknowledged it as a "State Standard" in accordance with NRS 378.255 (1).

ENDNOTES

¹ Nevada has well-established general rules of evidence that provide exceptions to the hearsay and best evidence objections, codified within Title 4 of the Nevada Revised Statutes (NRS) Chapters 47 to 56.

² The custodian affidavit format is referenced in NRS 52.260 (3)

³ See also Civil Practice Laws and Rules [CPLR], Rule 4520

⁴ NRS 51.135 and NRS 52.247

⁵ Courts may scrutinize untested technologies more rigorously than established ones, especially where there is no legal precedent.

⁶ The custodian affidavit format is referenced in NRS 52.260 (3)

⁷ For example, Nevada Information Technology Operations Committee (NITOC) has adopted Policies, Standards and Procedures (PSP's) that help ensure proper system controls are used to protect electronic recordkeeping systems and are available at <http://psp.state.nv.us/>

⁸ NITOC has adopted several PSP's that will help ensure security within an electronic recordkeeping system and are available at <http://psp.state.nv.us/>.

⁹ These are available on the NSLA's web site: <http://dmla.clan.lib.nv.us/docs/nsla/records/state.htm>

¹⁰ Available on the NSLA's web site: http://dmla.clan.lib.nv.us/docs/nsla/records/e_mail_policy.htm. Additional standards under the authority of DoIT and NITOC regarding use of the State e-mail system may be found at <http://psp.state.nv.us/>.

¹¹ The Guidelines are currently being revised. A current draft is available for review on-line at <http://dmla.clan.lib.nv.us/docs/nsla/records/edm2.htm>.

¹² TIFF: Tagged Image File Format. TIFF is a common format for exchanging raster graphics (bitmap) images between computer applications programs including those used for scanner images. A TIFF file can be identified as a file with a "tiff" or "tif" file name suffix. TIFF files are very common and are used to support most common graphic formats commonly used in desktop publishing, faxing, 3-D graphics applications, medical imaging and document imaging programs. A committee chaired by Aldus Corporation (now a part of Adobe) jointly developed the TIFF image format standard in 1986. Microsoft and Hewlett Packard contributed to the standard.

¹³ **Dated October 18, 2000 Available on-line at:**
http://www.archives.gov/records_management/policy_and_guidance/electronic_signature_technology.html

¹⁴ **NAC 239.630 "Long-term record" defined.** "Long-term record" means a record which must be retained for more than 6 years.

This document was produced by the Nevada Electronic Records Committee (NERC), a subcommittee of the Committee to Approve Schedules for the Retention and Disposition of Official State Records (NRS 239.073 et seq.), also known as The State Records Committee. NERC also serves as an advisory body to the Nevada State Historical Records Advisory Board (SHRAB) (NRS 378A) and to the Nevada Information Technology Operations Committee (NITOC). In existence since 2001, NERC's mission is to develop standards and guidelines for the creation, maintenance, accessibility, and long-term preservation of electronic records created and received by Nevada state and local governments.

**This publication may be printed or downloaded
from our Web Site at:**

<http://dmla.clan.lib.nv.us/docs/nsla/records/nerc/pdf/LegalRequirements.pdf>

