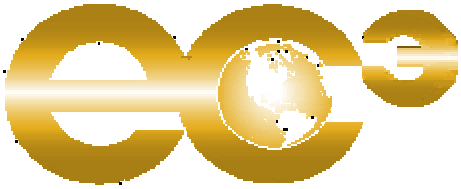
Electronic Records Management Guidelines for State Government

Ensuring the Security, Authenticity, Integrity, and Accessibility of Electronic Records



Exposure Draft

A National Electronic Commerce Coordinating Council *E-Sign Policy Workgroup Paper*

December 2001

National Electronic Commerce Coordinating Council

The National Electronic Commerce Coordinating Council (**NECCC**) is an alliance of national state government associations dedicated to the advancement of electronic government within the states. The Council is comprised of the National Association of State Auditors, Comptrollers and Treasurers (**NASACT**), the National Association of State Chief Information Officers (**NASCIO**), the National Association of State Purchasing Officials (**NASPO**), and the National Association of Secretaries of State (**NASS**). In addition to these voting members, other governmental and private organizations participate in an advisory capacity. These associations include the Information Technology Association of America (**ITAA**), the National Automated Clearing House Association (**NACHA**), the National Association of Government Archivists and Records Administrators (**NAGARA**), the National Association of State Chief Administrators (**NASCA**), the National Association of State Treasurers (**NAST**) and the National Governors Association (**NGA**). ITAA and NACHA represent private information technology companies and the financial services and technology industries.

NECCC Board

Chair: **Carolyn Purcell**, NASCIO, Texas CIO

Vice Chair: **Hon. J. Kenneth Blackwell**, NASS, Ohio Secretary of State

Secretary/Treasurer: **Richard B. Thompson**, NASPO, Maine Director of State Purchasing

Immediate Past Chair: **Hon. J.D. Williams**, NASACT, Idaho State Controller

NASACT	**Hon. Ralph Campbell, Jr.**, North Carolina State Auditor **Hon. Jack Markell**, Delaware State Treasurer
NASCIO	**David Lewis**, Chief Information Officer, Commonwealth of Massachusetts **Aldona Valicenti**, Chief Information Officer, Commonwealth of Kentucky
NASPO	**Dave Ancell**, Director, Office of Purchasing, Michigan Dept. of Management & Budget **Denise Lea**, Director, Louisiana Office of State Purchasing
NASS	**Hon. Mary Kiffmeyer**, Minnesota Secretary of State **Hon. Elaine Marshall**, North Carolina Secretary of State
ITAA	**Basil Nikas**, CEO, iNetPurchasing,com
NACHA	**William Kilmartin**, Accenture
NAGARA	**Terry Ellis**, Salt Lake County Records Management and Archives
NASCA	**Pam Ahrens**, Director, Idaho Department of Administration
NAST	**Hon. Jack Markell**, Delaware State Treasurer
NGA	**Thom Rubel**, National Governors Association

Acknowledgements

This white paper was prepared by the 2001 NECCC E-Sign Policy Workgroup, including the following authors: **John J. Aveni**, New York State Office for Technology; **Alan Kowlowitz**, New York State Office for Technology; and **Drew Mashburn**, Arkansas Office of Information Technology.

Table of Contents

BACKGROUND 3

STATEMENT OF BENEFITS: 3

PART 1: GENERAL CONCEPTS AND GUIDELINES 4

1.1 Identify and assess specific legal, business, and other requirements that apply to e-records 4

1.2 Base e-records management measures on the value of the records 4

1.3 Focus on the systems and business processes that produce e-records 5

1.4 Training is critical 5

PART 2: RECEIVING, CAPTURING AND CREATING E-RECORDS 5

2.1 Create or capture a record for each business transaction that complies with all legal or other requirements regarding the record's structure, content, and time of creation or capture. 5

2.2 Authenticate (prove the identity of) the sender of the record and make sure the e-record has not been altered. 6

2.3 Uniquely identify each record. 7

PART 3: MAINTAINING ACCESSIBLE, AUTHENTIC, AND COMPLETE E-RECORDS7

3.1 Maintain integrity of e-records as captured or created so that they can be accessed, displayed, and managed as a unit. 7

3.2 Retain e-records in an accessible form for their legal minimum retention periods as established in State Archives or local retention schedules. 8

3.3 Search and retrieve e-records in the normal course of business for all business uses throughout their entire legal minimum retention period. 10

3.4 Produce authentic copies of e-records and supply them in useable formats,including hard copy, for business purposes and all public access requirements. 11

PART 4: MAINTAINING SECURE, RELIABLE AND TRUSTWORTHY E-RECORDS SYSTEMS 12

4.1 Make sure the system performs in an accurate, reliable, and consistent manner in the normal course of business. 12

4.2 Protect e-records to enable their accurate and ready retrieval throughout their retention period. 14

4.3 Limit system access to authorized individuals and for authorized purposes. 14

SUMMARY GUIDELINES 16

WEB-AVAILABLE RESOURCES 18

GLOSSARY 19

Background

The NECCC E-Sign Policy Workgroup developed these practical guidelines to guide agencies toward developing effective electronic records management procedures. The guidelines provide a general direction on how state government agencies can ensure the authenticity, integrity, security, and accessibility of electronic records (e-records). Typically electronic records must meet the same requirements as their regular paper record counterparts. However, there are unique characteristics to electronic records management that this paper focuses on. While these guidelines were developed to assist state government agencies, private entities may find them equally useful in establishing their own electronic record systems.

Statement of Benefits

The drive to establish electronic government (e-government) in many states has begun to make electronic records (e-records) management an issue of vital concern. A key enabler of e-government is the establishment of a firm legal basis for and the ability to utilize and manage the electronic records created to conduct and document e-government transactions. The implementation of sound e-record management practices can address these issues as well as providing additional benefit such as:

- The creation and management of accurate and reliable e-records.
- Ensuring the legal acceptability of e-records.
- Reducing costs for records retrieval.
- Reducing reliance on paper records and the burden of paper record keeping.
- Ensuring long term access to e-records of enduring historical, legal, cultural, or administrative value.
- Improving citizen access to public information.
- Maintaining the confidentiality and privacy of non-public personal information.

Part 1 of the guidelines discuss key concepts and gives general guidance on how to manage e-records to ensure they are authentic, unmodified, accessible, and securely stored. Parts 2 through 4 provide guidance on the following topics:

- Receiving, Capturing, and Creating E-Records
- Maintaining Accessible, Authentic, and Complete E-Records
- Maintaining Secure, Reliable and Trustworthy E-records Systems

The subsection headings under each topic reflect what state agencies can do in order to create and maintain secure, authentic, and accessible e-records. These subsections are technology neutral and focused instead on achieving certain outcomes or performance standards. Long-term preservation solutions should be independent of media because media formats and standards will generally change during the retention period. Solutions need to focus on managing the records so that they are accessible and useable throughout their retention periods. Provided under each subsection is guidance on the policies, processes, and technological and physical measures that can help achieve the desired outcomes. The guidelines conclude with a table summarizing the guidelines and a "webography" of other relevant resources available on the Internet.

Part 1: General Concepts and Guidelines

1.1 Identify and assess specific legal, business, and other requirements that apply to e-records

The creation, format, and management of records are often based on specific legal mandates, business needs, and past practices. When contemplating the use of e-records, government agencies should assess their existing record keeping practices to determine which are based on:

- Legal mandates that must be met by the policies, procedures, and technology used to manage e-records.
- Business needs that should be addressed but can be modified or replaced when an e-records system is developed.
- Past practices in managing paper records that can be eliminated when an e-record system is developed.

State government officials should consult with their legal counsel and other knowledgeable staff to identify requirements relevant to e-records as soon as possible in developing e-records systems.

1.2 Base e-records management measures on the value of the records

Just as with paper records, the e-records a government agency produces or receives are **not** all of equal importance or value. Although all government records should be maintained properly, the effort and resources a state agency expends to manage and maintain records, including e-records, should be related to the records' value to the agency and the citizens it serves. The concept of risk management may be useful. Risk management requires: an analysis of risks, relative to potential benefits; consideration of alternative measures to address risks; and implementation of the measures that best address risk based on this analysis. In applying risk management to e-records, the following questions should be asked.

- What would be the impact on agency operations if the records were lost or otherwise unavailable?
- Would the agency or others suffer a financial loss if the records were unavailable?
- What is the likelihood that the records would be subject to or needed for a legal action? Would the inability to produce the records in a form admissible in court have a critical impact on the outcome of a case?
- Are the records required for an extended period of time?
- Do the records have significant cultural or historical value?

State government officials should bear in mind that the extent to which they achieve the outcomes outlined in these guidelines and the measures used to achieve them, is a business decision related to the value of the records in question to the government agency and the citizens of the state, the risk entailed if these records were unavailable and the cost to address the risk.

1.3 Focus on the systems and business processes that produce e-records

The reliability and accuracy of the processes and procedures used to create, capture, and maintain e-records are critical to demonstrating their authenticity, integrity and security. These factors are much more important than the format or medium of e-records or the specific technology used to create and maintain them. Government agencies should identify, specify and document these processes and procedures if they expect their e-records to be accepted in legal and other proceedings.

1.4 Training is critical

Training is particularly important in ensuring that staff adequately maintains systems used to create and maintain e-records. However, it is also important in ensuring that government officials are aware of the unique management issues raised by e-records due to the fragile media used to store them and the technology platform needed to access and use them. Government officials also need to be conscious of their responsibilities to manage e-records and diligently carry out these duties to ensure that e-records are admissible in legal proceedings and accessible throughout their legal retention periods.

Part 2: Receiving, Capturing and Creating E-Records

The systems supporting an agency function must be able to capture or create records in the required form, which includes required informational content and contextual elements (e.g., authorizations, date stamps, e-signatures). Records must also be identified when they are captured to support their accessibility. In transmitting and receiving e-records, precautions must be taken to prevent unauthorized persons from tampering with e-records and corruption of the records. Failure to do so could compromise the authenticity and integrity of the records.

2.1 Create or capture a record for each business transaction that complies with all legal or other requirements regarding the record's structure, content, and time of creation or capture.

Develop and document clear procedures and processes for the receipt, creation, processing, and filing of e-records: These policies and procedures should include acceptable record formats, as well as the point at which a transaction is completed and the record is securely stored so that it cannot be modified without detection.

Designate a receiving device: Government agencies need to designate a receiving device(s) for e-records. A "device" could mean a specific server but it also could be a specific e-mail address or website. A government should inform the public of what devices it has designated to receive e-records

2.2 Authenticate (prove the identity of) the sender of the record and make sure the e-record has not been altered.

Establish policies and procedures to authenticate senders and determine the integrity of each type of e-record: These policies and procedures establish the authenticity and integrity of the various types of e-records received by a government agency. These policies should be driven by the potential risk and costs if the records were tampered with, inappropriately disclosed, or otherwise compromised. Agencies should also develop and implement e-mail and Internet policies in conformance with their state's enterprise architecture.

Establish measures to secure transmission of e-records including the integrity of records during transmission and processing: These measures will vary with the level of risk, the business requirements, and the technology used. For example:

- Public Key Infrastructure (PKI), which provides a very strong encryption for higher risk transactions, can support electronic signatures as well as the following secure transmission measures.
    - Secure Sockets Layer (SSL) standard is often used for web-based applications. However, browsers must be PKI aware or enabled.
    - E-mail applications often use Secure Multipurpose Internet Mail Extensions (S/MIME).
- Pretty Good Privacy (PGP) is a technique for sending secure messages over a public network using a freeware encryption package available from the Massachusetts Institute of Technology.
- Virtual Private Network (VPN), which generally requires the same vendor's equipment at both endpoints, is used for ongoing business relationships via public networks.

Specific techniques may be used independently or in conjunction with the technology mentioned above to check if e-records have been altered. These can include such "low tech" measures as providing the sender with a receipt and copy of the received document, established data processing techniques such as edit checks and checksum, and hashing techniques, such as those used in digital signature technologies, that can easily detect changes to a record.

Maintain measures to authenticate the identity of the sender based on potential risk and legal requirements: This may vary based on the nature of the transaction and specific business requirements. Some transactions do not require authentication. Typically authentication is accomplished through the use of unique passwords and personal identifying numbers (PINs). Using unique user information such as mother's maiden name could enhance authentication. However, higher risk applications can rely on biometric identification (e.g., retinal scans, fingerprints, voice verification, signature dynamics) or electronic signature technologies that are often PKI-based.

Maintain measures to document the date and time of receipt: It is important to document this information for many government transactions, and this information is usually captured in an automated fashion by the receiving system. Receipt information should be attached or linked to the record received, as a time stamp would be on a paper record. For high-risk applications,

secure or trusted time-date stamping can be used where a neutral or trusted third party applies the electronic date and time stamp. A trusted time authority applies such electronic time stamps. Trusted time stamping is another service that can be provided within a PKI.

Confirm receipt: Some business processes or statutory mandates require that the receipt of documents be confirmed. Confirmation may take different forms depending on the type of application. For example, web-based applications may return a screen confirming a transaction along with a unique transaction number for tracking or auditing purposes. For high security environments, a separate confirmation via an alternative route is recommended. For example, a person's postal address could be confirmed via an external database and sent a confirmation via mail or courier (e.g. FedEx, UPS, etc.).

2.3 Uniquely identify each record.

Establish a method to uniquely identify each record: Minimal unique identifying identification data may include**:**

- Identification number or name
- Identity of record creator, information source or the owner (business unit)
- Date and time of receipt or creation
- Indexing information such as subject terms

Part 3: Maintaining Accessible, Authentic, and Complete E-Records

Government agencies are required to retain e-records to meet minimal legal retention requirements imposed by statute, or business or administrative needs. E-records with long term or permanent retention requirements must be preserved in an accessible and useable form by the agency or, in the case of state agencies, transferred to the appropriate entity (i.e. State Archives). Other e-records should be legally destroyed only under a records disposition authorization issued by the State Archives or other governing entity.

3.1 Maintain integrity of e-records as captured or created so that they can be accessed, displayed, and managed as a unit.

Maintain e-records management policy documenting the organization's policy on information management and storage: Policies should cover the following areas.

- **Specify what e-records are covered:** E-records should be grouped into "types" or "series" that can be managed in a consistent manner. For example information types may be specified either by reference to the business activity that created them (such as "vehicle registration," "public assistance case files," "fishing license file"), or to generic group (such as "accounting data," "customer documents," "manufacturing documents"). Some records will be more critical for agency operations, more likely to be needed for legal actions, or put the agency at risk if they were lost or not accessible. These records

should be afforded more management attention and a higher level of protection. This issue may already be addressed by existing record retention guidelines. However, even in states were records retention guidelines exist, they are frequently not applied to e-records.

- **Establish standards for file formats:** Policy should designate approved data file formats for each record "type." All information stored on a computer system requires software for retrieval and display. This software is subject to change, either by the implementation of new releases, or by changes to operating systems or hardware. A policy of approved media formats for records storage will facilitate data migration to ensure long-term retrieval of e-records.

- **Define responsibilities for information management functions:** An effective information policy needs to define responsibilities for implementing its various components. In the case of e-records, responsibilities will often be shared between program and technical staff as well as staff specifically assigned to records management functions.

- Define procedures for the storage and management of e-records to ensure access for the full length of their retention period. (See also section *4.1 Make sure the system performs in an accurate, reliable, and consistent manner in the normal course of business*)

Develop controlled storage or filing systems that maintain the integrity and accessibility of e-records: Once e-records are created or captured they need to be maintained in a controlled environment that can maintain their integrity and authenticity. This demands that e-records be stored in a secure, reliable and trustworthy e-records system as described in *part 4, Maintaining Secure, Reliable and Trustworthy E-Records Systems*. In addition, e-records must be stored so that any unauthorized change or modification can be prevented or at least detected. Document management or knowledge management products are available that can provide such solutions.

3.2 Retain e-records in an accessible form for their legal minimum retention periods as established in State Archives or local retention schedules.

- **Adopt and use records retention and disposition schedules in compliance with the appropriate records management state law(s)**: General schedules exist which cover the general functions of state agencies and all functions of local governments. State agencies can develop schedules for their unique functions following their respective procedures. An appropriate state entity may provide assistance for developing schedules and interpreting general schedules. This issue may already be addressed by existing record retention guidelines. However, even in states were records retention guidelines exist, they are frequently not applied to e-records.

Adopt and use state preferred technical standards and IT architecture: The preferred standards generally adhere to the open standards specifications of recognized national and

international standards bodies. Standards facilitate easier sharing of and access to e-records between similar systems.

Maintain e-records in encrypted form only as long as security concerns warrant: E-records are sometimes encrypted for security purpose during transmission over networks and during the course of a transaction. Highly sensitive records, such as those containing non-public personal information, may be stored in encrypted form for extended periods of time. However, the loss or destruction of a decryption key could result in the loss of access to encrypted records. Therefore, government agencies should avoid storing e-records in encrypted form beyond the point that security concerns warrant such a measure. The system security measures described in *Part 4, Maintaining Secure, Reliable and Trustworthy E-records Systems* should be sufficient to protect most e-records maintained by government agencies.

Develop retention solutions that best address an e-record's retention requirements: Any retention solution should address the required length of time records must be retained. For instance, records retained for only a short period of time (three to six years) could be maintained in the system that created or captured them for their entire retention period. However, any solution developed should accomplish the following:

- **Maintain the e-record's original functionality to the degree necessary:** Many e-records lose their meaning and usefulness if they can't be used or function as they did when they were in their original environment (e.g., ability to be processed or searched). Determine if it is necessary to retain an e-record's functionality. If so, the record should be retained in a format that can be processed or used by available technology.

- **Preserve the context and links between components of e-records**: In order to interpret the meaning of some e-records, all necessary file structures and relationships between record components need to be retained for the record's retention period. For example, a public key used to authenticate an electronically signed record or the link to a video file and the file that is part of a multimedia document might need to be retained for the record's retention period.

Develop solutions that can be applied with the least human intervention: A solution that is more automated is likely to be less labor intensive and more efficient, therefore increasing the likelihood that it will be implemented.

Develop solutions that are independent of media format and are technology neutral: Long-term preservation solutions should be independent of media because media formats and standards will generally change during the retention period. Solutions need to focus on managing the records so that they are accessible and useable throughout their retention periods.

Address long-term retention requirements and records preservation: Some e-records have very long or permanent retention requirements and the retention solution developed must preserve long-term access to them. Unfortunately, there is no easy technical solution to the long-

term retention of e-records. However, there are a number of approaches to the problem. The costs and benefits of any approach must be weighed along with continuing internal and external access needs. The various approaches to maintaining long-term access to e-records are described below.

Migration: System migration is the most commonly cited solution to preserving e-records. It requires the manager of an automated record keeping system to move e-records from an existing system to a more modern system before the original system becomes obsolete and inoperable. Migration should be implemented incrementally along with periodic system and software upgrades. It is a strategy often used in conjunction with maintaining e-records in a standard format.

- **Storing e-records in standard formats**: The use of standard formats (relational databases, ASCII, Portable Document Format, SGML, etc.) can help reduce the rate of technological obsolescence and the need for migration. However, this is not a permanent solution because standards change or are replaced over time. The National Institute of Standards and Technology is exploring the use of standard e-records storage formats.

- **Encapsulation**: Encapsulation refers to a method of capturing the look and feel of the original record along with any required metadata as a single digital object in a portable format. In some ways, encapsulation combines system migration with use of standard formats. Encapsulation strategies are just beginning to be investigated.

- **Conversion to other media**: It is relatively simple to output e-records to durable media such as paper or microfilm. E-records can be printed to paper or output directly to microfilm through computer-output microfilm (COM) and the paper or microfilm can be maintained as the preservation copy. This solution is only viable when all required metadata can be captured on the output media and where there will be no critical need to access or use the record in electronic form.

- **Emulating obsolete technology**: Emulation consists of using hardware and software to allow one computer technology to act as if it were another technology. This solution allows e-records to remain in their original file formats while the hardware and software change. Emulation is complicated and expensive to achieve for any sophisticated system. Research on emulation solutions is ongoing.

3.3 Search and retrieve e-records in the normal course of business for all business uses throughout their entire legal minimum retention period.

Maintain adequate search and retrieval capabilities to ensure that e-records can be retrieved for all legitimate business purposes for their full retention period: This should include retrieval during the period that records are stored on nearline or offline media. This will demand adequate indexing (*see part 2. Receiving, Capturing and Creating E-Records*) as well as search tools.

3.4 Produce authentic copies of e-records and supply them in useable formats, including hard copy, for business purposes and all public access requirements.

Develop or revise access and personal privacy protection policies to cover e-records: Such policies should be consistent with the requirements of the Federal Freedom of Information Act (FOIA), other state Freedom of Information laws and agency specific requirements.
Develop methods to provide public access to e-records and to protect personal privacy and confidentiality: When systems are designed, government agencies should develop methods of access that take into account the public access and confidentiality requirements. The need for public access to e-records must constantly be weighed against a government agency's legal obligation to protect personal privacy and confidentiality. For this reason government agencies must keep any private information confidential and develop automated means to redact or mask confidential information from e-records before releasing them to the public.

Collection and Use of Personal Information
The use of personal information collected, stored, or disseminated by government for purposes other than those purposes to which a person knowingly consents can seriously endanger a person's right to privacy and confidentiality.

a. Personal information should be:
    i. Collected, used and maintained only as expressly authorized by law and for legitimate public purposes;
    ii. Relevant to and used only for the specified purpose for which it was originally collected;
    iii. Used only if accurate and up-to-date;
    iv. Kept secure; and
    v. Retained only as long as necessary and then destroyed.
b. There is current debate concerning selling and releasing personal information for commercial purposes. Both federal and state laws can impact policies and practices addressing these issues. Consequently, agency legal counsel should keep up to date on legal developments with these issues.
c. The ability to electronically store, retrieve, and aggregate information raises new concerns about the potential for personal information to not only be accessed, but mined and distributed, as well.
d. Agencies collecting, maintaining or using personal information, under its control, should take precautions to prevent its misuse. It may be an unwarranted invasion of personal privacy for an agency to make personal information available to the public.
e. Social Security numbers, bank account numbers, and credit card numbers should be confidential and should be redacted from any record that could be subject to public scrutiny. State agencies should abide by existing laws prohibiting such information from being released.
f. Several states have authorized by law that personal information shall not be shared among government entities without the consent of the affected individuals. Some state laws mandate that agencies that enter into contracts or agreements for sharing

personal information with other entities must incorporate requirements into such contracts or agreements that protect the information from inappropriate uses.

g. Several states have mandated by law or policy that when personal information about individuals is collected, the individuals shall be notified by the collecting agency that the law may require public disclosure of the information, or its dissemination to other agencies, through the state's open/public record laws or by court order. If personal information is collected via e-mail and Web-based forms, laws and/or policies may exist for an individual to opt-out from having their personal information shared with another party, and/or allowing the individual to access their personal information and correct the same. Such laws and/or policies must be considered by states when designing and implementing effective electronic records management procedures.

Provide access to e-records in the form the user prefers: Some people do not have access to the technology needed to use e-records or prefer records in paper form. Some state e-record management regulations may require government agencies to provide access to e-records in paper form if requested. This does not mean that governments must maintain paper copies of e-records, only that they have the technical capability to generate copies of e-records in both paper and electronic form.

Part 4: Maintaining Secure, Reliable and Trustworthy E-Records Systems

The acceptance of e-records for legal, audit, and other purposes is contingent on establishing their authenticity and reliability by demonstrating the trustworthiness of the system used to produce them. Systems that produce records must be shown to do so in the normal course of business and in an accurate and timely manner. The following suggestions should assist record keepers in their efforts to maintain authentic and reliable e-records that can be successfully used for these purposes.

4.1 Make sure the system performs in an accurate, reliable, and consistent manner in the normal course of business.

Define and document system management policies and procedures: Written policies and procedures for each system should:

- Describe the methods used to create, modify, duplicate, and destroy records.
- Define the roles and responsibilities of the individuals involved in records creation, maintenance, and destruction.
- Provide for consistent quality control, problem resolution, and other activities that might be subject to inconsistent action or misinterpretation.
- Demonstrate the purpose and uses of the system.
- Be kept up-to-date and readily available.

Assign system management roles and responsibilities, and implement the principle of separation of duties implemented pursuant to written policies: *Separation of duties* refers to dividing roles

and responsibilities so that a single individual cannot subvert a critical process. For example, in financial systems, no single individual should be given authority to issue checks. Rather, one person initiates a request for a payment and another authorizes the payment. Another example would be to ensure that more than one person be delegated the task of purging outdated electronic files.

Develop and maintain problem resolution procedures including incident reporting and response procedures: These can help ensure that a system's problems are quickly identified, attended to and resolved. They, along with operation logs and a help desk can help document that problems didn't jeopardize the integrity of the system and its e-records.

Test system performance including the reliability of hardware and software: The reliability of hardware and software affects the authenticity and integrity of e-records. Equipment malfunctions can alter the content of e-records. If data processing equipment and software used to store and produce e-records is not reliable, the integrity of the records may be challenged. The integrity of e-records can be enhanced by:

- Routinely testing hardware and software as well as performing maintenance in accordance with the manufacturer's advice.
- Retaining documentation related to hardware and software procurement, installation, and maintenance.
- Maintaining operation logs and run schedules to document the reliability of system operation and performance.

Government agencies should consider an external technical evaluation (or audit) of their high-risk systems. An independent verification of such systems could document the reliability of the systems and the e-records they produce as well as increase public confidence in them.

Maintain audit trails of system activity by system or application processes and by user activity: In conjunction with appropriate tools and procedures, audit trails can provide a means to help accomplish several security-related objectives, including individual accountability, reconstruction of events, intrusion detection, and problem identification. An audit trail should include sufficient information to establish what events occurred and who (or what) caused them. It can be used to document the trustworthiness and reliability of a system as well as the integrity of the e-records stored in the system. If possible, audit trails should be generated automatically by the system receiving, processing, and maintaining the records. All audit records should be retained in compliance with established State or local government records retention and disposition schedules.

Provide training and user support adequate to ensure users will implement system procedures: Formal training and support programs help ensure that staff understand and implement policies and procedures. Instructions for data input, processing, and retrieval support staff training and document the agency's efforts to train staff. Documentation showing that the agency provided sufficient supervision to oversee staff in the system's proper use and maintenance will also strengthen the case that procedures were followed. It is also advisable to keep records of attendance at training sessions and certification of training.

4.2 Protect e-records to enable their accurate and ready retrieval throughout their retention period.

Develop a contingency plan that includes data backup, disaster recovery, and emergency operations: Contingency plans can help government agencies quickly put back into operation systems after a disaster. The plans should include data backup and recovery to prevent the loss of e-records.

Establish controls for the accuracy and timeliness of input and output: The accuracy and timeliness of input and output of systems is critical to demonstrating the integrity and authenticity of the e-records produced by the system.

Implement media controls: Various measures, such as standard labeling and maintaining tracking logs, provide physical and intellectual control over tapes, diskettes, and other media. Offline media should also be stored in environmentally and physically controlled locations. The extent of media control depends upon many factors, including the type of data, the quantity of media, and the nature of the user environment. Media used to store critical or high-risk e-records will normally demand higher-levels of control than other data.

Perform routine backups: It is critical to backup software and data especially if that data constitutes e-records. Frequency of backups will depend upon how often data changes and the importance of those changes. Program managers should be consulted to determine what backup schedule is appropriate. Backup copies should be tested to determine if they are usable and stored securely at a location away from the system in the event of a disaster.

4.3 Limit system access to authorized individuals and for authorized purposes.

Maintain physical and environmental security controls: Physical and environmental threats can have an impact on e-records, especially those stored on fragile offline media. An organization's security program should address physical access and appropriate environmental conditions in office space, data centers, or rooms containing hardware (such as local area network (LAN) server), system wiring, supporting services (e.g., electric power), backup media, and any other system elements. The program also needs to address threats such as fires, utility failures, structural collapse, and plumbing failure.

Provide for identification and authentication: These are technical measures that are designed to prevent unauthorized people (or unauthorized processes) from entering a system. Not only are these significant in transactions over networks, as discussed above, but also they are also important in managing systems and ensuring the security of e-records. System should be able to identify and differentiate between users through a unique user ID and to link each activity on a system to a specific user through an ID. IDs should belong only to currently authorized users. Authentication is the means of establishing the validity of a user's identity. There are three means to authenticate a user's identity, which can be used alone or in combination:

- **Something that only the individual knows:** A secret (e.g., a password, Personal Identification Number (PIN), or cryptographic key).
- **Something the individual possesses:** A token (e.g., an ATM card or a smart card).
- **Something the individual is**: A biometric (e.g., characteristics such as a voice pattern or a fingerprint).

Maintain logical access control: Access is the ability to do something with a computer resource (e.g., use, change, or view). Logical access controls are the system-based means by which the access is explicitly enabled or restricted in some way. They can prescribe who can have access to a specific system resource and the type of access that is permitted. In general, organizations should base access control policy on the principle of least privilege. *Least privilege* refers to granting users only the system access needed to perform their official duties. Data entry clerks, for example, may not have any need to run analysis reports of their database. Organizations should control access to resources based on the following access criteria, as appropriate:

- **Identity (user ID):** In order to support individual accountability.
- **Roles:** Such as the users job assignment or function.
- **Location:** Based upon physical or organizational unit.
- **Time:** Such as time-of-day and day-of-week restrictions on access. For example, use of confidential personnel files may be allowed only during normal working hours.
- **Transaction:** For example, access to a case file could be granted only for the duration of a transaction (e.g., re-certification of benefits). A caseworker would be given read access to the case file. When the transaction is completed, the access authorization is terminated.

Maintain external access control mechanisms: These are a means of controlling interactions between the system and outside people, systems, and services. When setting up access controls, organizations should consider the following mechanisms:

- **Encryption:** Encrypted information can only be decrypted and read by those possessing the appropriate cryptographic key.

- **Secure gateways or firewalls:** Secure gateways block or filter access between two networks, often between a private network and a larger, more public network such as the Internet. Secure gateways allow internal users to connect to external networks while protecting internal systems.

- **Host-based authentication:** Host-based authentication grants access based upon the identity of the host originating the request, instead of the identity of the user making the request. Many network applications in use today use host-based authentication to determine whether to allow access.

Summary Guidelines for Ensuring the Security, Authenticity, Integrity, and Accessibility of Electronic Records

General Guidelines	
Identify and assess specific legal, business, and other requirements that apply to e-records ***Base e-records management measures on the value of the records*** ***Focus on the systems and business processes that produce e-records*** ***Training is critical***	
Receiving, Capturing and Creating E-Records	
Outcomes	**Implementations**
Create or capture a record for each business transaction that complies with all legal or other requirements regarding the record's structure, content, and time of creation or capture	Develop and document clear procedures and processes for the receipt, creation, processing, and filing of e-records Designate a receiving device
Authenticate (prove the identity of) the sender of the record and make sure the e-record has not been altered	Establish policies and procedures to authenticate senders and determine the integrity of each type of e-record Establish measures to secure transmission of e-records including the integrity of records during transmission and processing Maintain measures to authenticate the identity of the sender based on potential risk and legal requirements Maintain measures to document the date and time of receipt
Uniquely identify each record	Establish a method to uniquely identify each record
Maintaining Accessible, Authentic, and Complete E-Records	
Outcomes	**Implementations**
Maintain integrity of e- records as captured or created so that they can be accessed, displayed, and managed as a unit	Maintain e-records management policy documenting the organization's policy on information management and storage Develop controlled storage or filing systems that maintain the integrity and accessibility of e-records
Retain e-records in an accessible form for their legal minimum retention periods as established in state or local retention schedules	Adopt and use records retention and disposition schedules in compliance state and local law Adopt and use state preferred technical standards Maintain e-records in encrypted form only as long as security concerns warrant Develop retention solutions that best address an e-record's retention requirements
Search and retrieve e-records in the normal course of business for all business uses throughout their entire legal minimum retention period	Maintain adequate search and retrieval capabilities to ensure that e-records can be retrieved for all legitimate business purposes for their full retention period

Produce authentic copies of e-records and supply them in useable formats, including hard copy, for business purposes and all public access requirements	Develop or revise access and personal privacy protection policies to cover e-records Develop methods to provide public access to e-records and to protect personal privacy and confidentiality Provide access to e-records in the form the user prefers
Maintaining Secure, Reliable and Trustworthy E-Records Systems	
Outcomes	**Implementations**
Make sure the system performs in an accurate, reliable, and consistent manner in the normal course of business	Define and document system management policies and procedures Assign system management roles and responsibilities, and implement the principle of separation of duties implemented pursuant to written policies Develop and maintain problem resolution procedures, including incident reporting and response procedures Test system performance including the reliability of hardware and software Maintain audit trails of system activity by system or application processes and by user activity Provide training and user support are adequate to ensure users will implement system procedures
Protect e-records to enable their accurate and ready retrieval throughout their retention period	Develop a contingency plan that includes data backup, disaster recovery, and emergency operations Establish controls for the accuracy and timeliness of input and output Implement media controls Perform routine backups
Limit system access to authorized individuals and for authorized purposes	Maintain physical and environmental security controls Provide for identification and authentication Maintain logical access control Maintain external access control mechanisms

Web-Available Resources

Association of Records Managers and Administrators

Association for Information and Image Management

Center for Technology in Government, University at Albany, *Models for Action: Developing Practical Approaches to Electronic Records Management and Preservation*

Commission on Preservation and Access, Magnetic Tape Storage and Handling

Joint Interoperability Test Command, DISA, DoD, Records Management Application (RMA) Certification Testing

National Institute of Standards and Technology, NIST Computer Security Special Publications

National Archives and Records Administration (NARA) Fast Track Guidance Development Project (To identify currently available "best practices" and provide guidance quickly on electronic records issues that urgently confront Federal record keepers)

Arkansas: Practical Guide to Electronic Records Management: http://www.oit.state.ar.us/Arch/dwnlds/RecordMgtGuideline_v1_.pdf

Arkansas: Managing Email Guidelines: http://www.oit.state.ar.us/Arch/dwnlds/E-Mail_Mgmt.pdf

California's E-Record Guidelines: http://www.pd.dgs.ca.gov/materials/hbtabl.asp

Kansas Electronic Commission: http://da.state.ks.us/itab/erc/

Kansas Electronic Records Guideline: http://www.kshs.org/archives/ermguide.htm#intro

Delaware Public Archives: http://www.kshs.org/archives/ermguide.htm#intro

New York State Office for Technology: Electronic Signature and Records Act (ESRA) Guidelines: E-Signature Performance, E-Signature Security, E-Records http://www.oft.state.ny.us/esra/Guidelines_files/index.htm

New York State Archives' Guidelines Most Relevant to E-Signatures and E-Records http://www.sara.nysed.gov/pubs/lgrtip.htm#erm

North Dakota E-Records Guidelines: http://www.state.nd.us/itd/records/doc/erguide.pdf

Minnesota: Preserving and Disposing of Public Records: http://www.ipad.state.mn.us/

Utah State Archives and Records Service: http://www.archives.state.ut.us/recmanag/electronic.htm

Glossary

Accessibility - is the attribute of records or information being available for appropriate use over time. For e-records accessibility includes having the technical means and metadata (data describing how, when, and by whom an e-record was created, and how it is formatted) to access, use, and understand the records.

Alphanumeric - Describes the combined set of all letters in the alphabet and the numbers 0 through 9. It is useful to group letters and numbers together because many programs treat them identically, and differently from punctuation characters. For example, most operating systems allow you to use any letters or numbers in filenames but prohibit many punctuation characters. Your computer manual would express this rule by stating: "Filenames may be composed of alphanumeric characters."

Asymmetric cryptography or crypto-system - A system of cryptography that employs two computationally related alphanumeric usually known as a key pair. A private key, known only to the holder, is used to create an e-signature or decrypt, and the other or public key known to others is used to verify the e-signature or encrypt.

Authenticity - refers to the methods used to verify the source or origin of an e-record. Authenticity is closely related to the concept of ***integrity***.

Biometrics - In computer security, biometrics refers to authentication, techniques that rely on measurable physical characteristics that can be automatically checked. Examples include computer analysis of fingerprints or speech.

Checksum - A simple error-detection scheme in which each transmitted message is accompanied by a numerical value based on the number of set bits in the message. The receiving station then applies the same formula to the message and checks to make sure the accompanying numerical value is the same. If not, the receiver can assume that the message has been garbled.

Cryptographic - Related to cryptography which is (i) The mathematical science used to secure the confidentiality and authentication of data by replacing it with a transformed version that can be reconverted to reveal the original data only by someone holding the proper cryptographic algorithm and key. (ii) A discipline that embodies the principles, means, and methods for transforming data in order to hide its information content, prevent its undetected modification, and/or prevent its unauthorized uses.

Cryptographic keys – Data used to encrypt or decrypt a message or information.

Electronic record - means any record created, stored, sent or received in a non-tangible form, including by or relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities. Source: Adapted from *UETA* Sections 102(5) (definition of "electronic") and 102(7) (definition of "electronic record"), and the Reporter's Note to Sec. 102(5).

Hashing - Producing *hash values* for accessing data or for security. A hash value (or simply *hash*) is a number generated from a string of text. The hash is substantially smaller than the text itself, and is generated by a formula in such a way that it is extremely unlikely that some other text will produce the same hash value. Hashes play a role in security systems where they're used to ensure that transmitted messages have not been tampered with. The sender generates a hash of the message, encrypts it, and sends it with the message itself. The recipient then decrypts both the message and the hash, produces another hash from the received message, and compares the two hashes. If they're the same, there is a very high probability that the message was transmitted intact.

Integrity - is the attribute that the record's contents have not been changed, deleted or otherwise altered. In addition, integrity addresses the accuracy and timeliness of the contents of a record. Both authenticity and integrity are derived from the legal arena and have a strong bearing on the legal admissibility of records.

Pretty Good Privacy (PGP) - A technique for encrypting messages developed by Philip Zimmerman. PGP is one of the most common ways to protect messages on the Internet because it is effective, easy to use, and free. PGP is based on the public-key method, which uses two keys -- one is a public key that you disseminate to anyone from whom you want to receive a message. The other is a private key that you use to decrypt messages that you receive. To encrypt a message using PGP, you need the PGP encryption package, which is available for free from a number of sources. The official repository is at the Massachusetts Institute of Technology.

Plaintext - In cryptography plain text refers to any message that is not encrypted and therefore easily read and understood.

Private key - A cryptographic key kept secret or known only by the holder. Private keys can be used to create e-signatures or decrypt messages or files. The same private key used to sign should not be used to decrypt.

Public Key Infrastructure (PKI) - The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a certificate-based asymmetric cryptographic system. The PKI consists of systems that collaborate to provide and implement e-signatures, encryption, and authentication services.

Security - refers to the protection of information assets, including both physical and technical controls over access to information. Security has technical, physical, and procedural components.

Secure Sockets Layer (SSL)- This is a protocol developed by Netscape for transmitting private documents via the Internet. SSL works by using a private key to encrypt data that's transferred over the SSL connection. Both Netscape Navigator and Internet Explorer support SSL, and many Web sites use the protocol to obtain confidential user information, such as credit card numbers. By convention, Web pages that require an SSL connection start with *https:* instead of *http*:. SSL has been approved by the Internet Engineering Task Force (IETF) as a standard.

Smart card - A hardware token that incorporates one or more integrated circuit (IC) chips to implement cryptographic functions and that possesses some inherent resistance to tampering.

S/MIME - Short for *Secure/MIME,* a new version of the MIME protocol that supports encryption of messages. S/MIME is based on RSA's public-key encryption technology. It is expected that S/MIME will be widely implemented, which will make it possible for people to send secure e-mail messages to one another, even if they are using different e-mail clients.

Tokens - A small hardware device used for security purposes to store confidential user identification or authentication information such as a ***private key***.

Trustworthy system - Computer hardware, software, and procedures that are reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy. A trustworthy system is not necessarily a "trusted system" as recognized in classified government nomenclature.

Virtual Private Network (VPN) - A *network* that is constructed by using public wires to connect nodes. For example, there are a number of systems that enable you to create networks using the Internet as the medium for transporting data. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted.