NEW YORK STATE OF OPPORTUNITY. | Office of Information Technology Services

State Capitol P.O. Box 2062
Albany, NY 12220-0062
www.its.ny.gov

New York State Information Technology Guideline	**No:** NYS-G04-001
IT Guideline: **Electronic Signatures and Records Act (ESRA)**	**Updated:** 05/04/2021
	Issued By: NYS Office of Information Technology Services **Owner:** Division of Legal Affairs

1.0 Purpose and Benefits

This best practice guideline:

- explains the definition of an e-signature under the ESRA law; and
- advises on choosing e-signature solutions meeting business and legal needs, while ensuring e-record authenticity, integrity, security, and accessibility.

2.0 Authority

NYS Technology Law and *Section 2 of Executive Order No. 117,* established January 2002, provide the NYS Chief Information Officer and NYS-ITS authority to oversee, direct, and coordinate the establishment of information technology policies, protocols, and standards for State government, including hardware, software, security, and business re-engineering. Details about this authority are found in *NYS ITS Policy NYS-P08-002, Authority to Establish State Enterprise Information Technology (IT) Policy, Standards and Guidelines.*

3.0 Scope

This best practice guideline applies to all "governmental entities" as defined under ESRA § 302(5) as: *"any state department, board, bureau, division, commission, committee, public authority, public benefit corporation, council, office, or other governmental entity or officer of the state having statewide authority, except the state legislature, and any political subdivision of the state."* Private individuals and entities may also find these ESRA Guidelines useful.

4.0 Information Statement

4.1 Introduction

ESRA's purpose is to facilitate e-Commerce and e-Government in New York State by giving electronic signatures and records (e-signatures and e-records) the same force and effect as signatures and records produced by non-electronic means.[1] In most cases, the use and acceptance of e-signatures or e-records is completely voluntary, as ESRA does not require private parties or governmental entities to use or accept e-signatures or e-records, unless some other law provides otherwise. The ESRA Guidelines are designed for governmental entities, but private individuals and entities may also find them helpful. ESRA regulatory changes or other developments may be noted on ITS' webpage: https://its.ny.gov/electronic-signatures-and-records-act-esra.

Unless otherwise provided by law, governmental entities that use e-records must:

- Allow citizens to access records as permitted by law.
- Provide, or accept for submission or filing, hard copy paper documents; and
- Not require submission or filing of records electronically.

All laws applicable to government records are applicable to e-records, including retention, accessibility, and disposition requirements under the Arts and Cultural Affairs Law, the Judiciary Law, or local statute. Governmental entities that use and accept e-records must also ensure their authenticity, integrity, and security and, when appropriate, their confidentiality (see Title 9 NYCRR Part 540.5(d)).

The definition of "electronic signature" in ESRA § 302(3) conforms to the definition found in federal law (the "E-Sign" Act), affording the parties to an electronic transaction maximum flexibility in selecting an appropriate e-signature solution.

ESRA-related amendments periodically occur, such as under Chapter 549 of the Laws of 2011, when ESRA and the NYS Real Property Law were amended to allow local recording officers to choose using e-recording of instruments affecting real property, or, through Executive Orders during the COVID-19 pandemic in 2020.[2] In its ESRA role as "electronic facilitator," ITS not only provides direct ESRA guidance when asked, but also periodically updates its website, its regulations, and these ESRA Guidelines to ensure relevance to statutory and other amendments and technological changes.

---

[1] ESRA § 307 contains exceptions such as for documents "providing for the disposition of an individual's person or property," or for "negotiable instruments." ITS as ESRA's "electronic facilitator" can exempt other types of records but has not done so to date.

[2] In 2020, NYS Executive Order No. 202.7 temporarily authorized NYS notarial acts to be performed utilizing audio-video technology, as well as allowing e- signatures to be used to execute documents and forms authorizing or accepting funeral services.

These guidelines are organized into two major sections concerning:

- **E-signature Guidelines,** describing ESRA's definition of an e-signature and ways to select e-signature solutions meeting business and legal needs); and
- **E-records Guidelines**, describing ways to ensure e-records' authenticity, integrity, security, and accessibility, including when electronically signed.

4.2 E-signature Guidelines

4.2.1 Overview of the Business and Legal Function of a Signature: A signature can serve several business and legal purposes, demonstrating: intent (a signature on a signed document identifies the signer and an understanding and intent to carry out what was stipulated); authentication and approval (linking the signer with the signed document provides evidence the signer saw and acted to approve or authorize it); security (signatures may protect against fraud, impersonation, or intrusion, and can impart clarity and finality to the transaction reducing later need to inquire beyond the face of a document); and ceremony (signing is a meaningful act warning the signer that by approving the document, the signer may be making a legally binding commitment).

4.2.2 Is an E-signature is Needed or Desirable? Review business and legal requirements, and transactional risks. Creating and maintaining e-signed, e-records may require more resources/effort than unsigned e-records. Consider:

Is a signature legally required? Specific federal, state, and local laws and regulations require signatures for various transactions. Under the statute of frauds, to be enforceable certain contracts and documents must be in writing and/or signed.

Is there a business need for a signature? Even if not legally mandated, signatures may be used on paper documents for purposes such as authentication or security, e.g. for documenting that a party to a transaction attested to the accuracy of the information provided, agreed to certain conditions, and/or read and understood related documents. In e-transactions where no formal signature is legally required, it may be preferable to address authentication and security using technologies and procedures meeting business needs without using an e-signature. However, higher risk transactions may carry legal implications or otherwise benefit from using e-signatures for system security, audit, fraud protection, repudiation, or program management issues. Consult legal counsel to review such issues and before deciding to implement an e-signature solution.

4.2.3 ESRA Definition of an Electronic Signature: ESRA, at §302 (3), defines an “electronic signature” as: "an electronic sound, symbol, or process, attached to or logically associated with an electronic record and executed or adopted by a person with the intent to sign the record." This definition affords the parties to an e-transaction the greatest possible flexibility in selecting an appropriate e-signature solution, while setting some parameters on what constitutes an e-signature for purposes of ESRA:

"[A]n electronic sound, symbol, or process. . .": Under ESRA, various digital objects may serve as e-signatures, as simple as a set of keyboarded characters or complex as an encrypted hash of a document's contents. ESRA also allows a process to create an e-signature, when a system used to create a signed e-record associates the recorded events of accessing an application with the content to be signed, creating a virtual record of the signer's actions and intent. Such signing processes may also use a password, PIN, or other digital object to authenticate the signer.

"[A]ttached to or logically associated with . . .": A penned signature becomes part of a physical paper document and remains with it during transit and after filing. Under ESRA, e-signatures are viewed as "attached to or logically associated with an electronic record" if the e-signature is linked to the record during transmission and storage, achieved by various means. For instance, an e-signature can be a discrete digital object that is part of the document the same as for an ink signature, or, can be an object associated with the document through an embedded link, or be maintained separately but logically associated with the record through a database, index, or other means.

When a process serves as an e-signature, the system used to create a signed e-record logically associates all the signed record's components, e.g. when a document is created with an official's sign-on to a procurement system where the official has only been authorized to access the system to create signed procurement documents, and the official's authority to sign is embedded in the system. The record is created through a sign-on authentication using a PIN or password with the official's actions captured while accessing the system. The record exists conceptually as a 'document' in the system, but the various pieces of the "record" may be maintained in various databases and system logs. The collection and maintenance of different informational pieces, along with the official's intent to sign the record, creates an e-signature under ESRA.

Under ESRA the attachment or logical association between signed record and signature must be created at the point a record is signed, maintained during transmission of the signed record, and retained as long as the signed record is needed including subsequent storage. Creation of the e-signature, including its attachment or logical association to the signed record, can occur outside the government entity's system. A private sector entity regularly submitting reports to a government agency might have an internal system housing and formatting electronic reports, with an authorized signer e-signing such reports at one point in time, and a government entity electing to accept those signed reports when they are later electronically submitted later.

"[E]xecuted or adopted by a person with intent to sign the record.": Generally, a signature is a ceremonial act identifying the signer and conveying a commitment to carry out stipulations in the signed document. Under ESRA, while e-signatures must show the same intent as signatures affixed by hand, ESRA doesn't require any specific

level or method of signer identification ("ID") or authentication, so government entities are free to select such methods as meet their needs. Selecting an appropriate identification and authentication approach is one consideration in selecting an e-signature solution.

A signer's intent can be captured in many ways, such as automatically captured and documented by the signer's actions after entering an information system. But to avoid confusion as to signer intent, rather than rely solely on system recordation, government entities might adopt a number of other simple practices:

- Prior to applying an e-signature, afford the signer an opportunity to review the entire document or content to be signed.
- Make it impossible for an e-signature to be applied to a document without the signer having been informed that a signature is being applied.
- Format e-signed records to contain similar signature elements as in paper records so a reader may readily identify the significance of the signature at the bottom.
- Allow the signer's intent to be expressed as part of the record or in a certification statement submitted with and linked to the signed record.
- Require the signer to act affirmatively to indicate assent to the document being signed, such as requiring the signer to click an "Accept" button, choose between that and a "Reject" button to show that a choice was made, or alternately be required to type specific words of acceptance (e.g., "I ACCEPT" or "I AGREE").
- Record the date, time, and fact that the signer indicated his or her intent and retain this information for evidentiary purposes. This may be different than the time the signer accessed the application or was authenticated.

Below is an example of a generic signature attestation/affirmation statement that can be modified for use with specific e-signature applications.

I agree, and it is my intent, to electronically sign this document by (describe the e-signature solution used). By submitting this e-document to (name of recipient individual or entity) in this way, I understand that my e-signing and submitting is the legal equivalent of having placed my handwritten signature and affirmation on the submitted document, and am affirming to the truth of the information contained therein.

Some commercial e-signature products provide a "ceremony" warning a signer that a legally binding commitment is being made, collect contextual information about the circumstances of the signing, provide formats and visual signatures similar to those found in paper documents, and collect information concerning the signer's intent.

4.2.4 E-signature Approaches: E-signature creation involves varied technologies, credentials/digital objects, and processes. Instead of stand-alone technologies, envision a range of e-signing approaches with varying levels of protection (security, authentication, record integrity, and repudiation). The descriptions below are roughly organized from lowest to highest protection levels, which can be combined to increase

protection strengths. Governments selecting from these e-signature approaches or combinations must weigh factors such as public policy and legal concerns:

- **Click Through/Click Wrap:** Signers are asked to affirm intent or agreement by clicking a button, sometimes typing "I agree" before clicking to guard against later claims of errors. Identification information collection, authentication processes before the signature is applied, and signing process security procedures can vary greatly. Click Through/Click Wrap is mostly used for low risk, low value consumer transactions, sometimes combined with approaches using Personal Identification Numbers (PINs) and/or passwords to authenticate signers.

- **S-signatures:** Simple symbols between forward slash marks ("/ s /") used by some government agencies to avoid identity theft risk or misuse, especially when posted on publicly accessible Internet sites. The USPTO, federal Department of Health and Human Services, Idaho courts, and California Division of Workers' Compensation all use S-signatures.[3] If an S-signature meets ESRA's other indicia of an e-signature, it has the same validity as any other e-signature.

- **PIN or password:** Application access may require entering identifying information such as ID number, name, or "shared secret" (known to both the user and the system), such as PIN and/or password. The system confirms the PIN/password is associated with that person and "authenticates" them.[4] The level of security varies depending on the transaction's risk or value. Low risk/low value transactions may require minimal, often unverified identifying information, while for higher risk transactions the application sponsor might only issue a PIN after an ID process applying rigorous personal information verification procedures.

- **Digitized Signature:** A graphical image of a handwritten signature, often used in face-to-face consumer credit card transactions with the signature rarely validated, sometimes created using a special computer input device such as digital pen and pad. Signature validation may compare the digitized signature representation with a stored copy. This has similar security issues as PIN or password, as the digitized signature is another form of shared secret known both to the person and to the system. Forging digitized signatures can be more difficult than forging paper signatures as the technology comparing the submitted signature image with the known signature image is more accurate than the human eye.

- **Signature Dynamics:** In this digitized signature variation each pen stroke is measured (e.g., duration, pen pressure, size of loops, etc.), creating a metric to compare to a reference value created earlier, thus authenticating the person

[3] See: USPTO, 37 CFR 1.4(d)(2)); DHHS, "Standard and Usability Guideline for Signatures"; Idaho courts ("Order Amending Rule on Electronic Filing and Service); and California Division of Workers' Compensation ("Electronic Adjudication Management System").

[4] Some more secure approaches may require entering personal information such as name, date of birth, or sex with the PIN and password. NYS agencies seeking to collect such personal information must comply with the obligations and requirements of the NYS Personal Privacy Protection Law (Public Officers Law, Article 6-A).

signing. These measurements can be combined with techniques used to create a digital signature, ensuring document integrity and more reliable signer authentication.

- **Biometrics:** Unique physical characteristics can be converted into digital form interpreted by a computer.[5] A microphone, optical reader, or other device measures the biometric, comparing it to a profile of one authenticated and stored beforehand. With software acceptance of a match, the transaction may proceed. Improving biometric applications may provide high authentication levels but are not foolproof and may result in false positives or negatives.[6]

- **Shared Private Key (Symmetric) Cryptography:** Shared between the e-transaction host and the signer, this verifies identity when e-signing a document using a single cryptographic key not publicly known, often a small secured hardware device (e.g. RSA SecureID), whose symmetric key intermittently generates and displays "one time" passwords, typically inputted from the device to a computer, along with a PIN. The key isn't really "private" to the signer and hence has lesser authentication value but can be made more secure through the use of standards-based encryption techniques and smart cards or other hardware tokens.

- **Public/Private Key or Asymmetric Cryptography:** Two mathematically linked keys are generated, one a publicly available validation key, the other a private key that can't be deduced from the public key. The public key is often part of a "digital certificate", a digitally signed e-document binding the individual's identity to an unalterable private key. The signer creates a "digital signature" when using the private signing key, creating a unique mark (called a "signed hash") on an e-document. The document recipient uses the signer's public key to authenticate the attached private key and verify the e-document was not altered after signing. These are often used within the context of a Public Key Infrastructure (PKI) in which a trusted third party known as a Certification Authority (CA) binds individual to private keys and issues and manages certificates. A PKI is governed by a certificate policy that governs all aspects of a digital certificate's generation, management, use, and storage as well as the roles and responsibilities of all entities involved in the PKI.

- **Microchip Devices:** While not a separate e-signature approach in itself, using an embedded microchip generating, storing, and/or processing data for identification (such as small plastic smart cards, USB drives, or chipped watches/phones), these can support various authentication and e-signature approaches. The device is read contact-less by a radio frequency reader or inserted into a computer or network microchip detector. The device's chip is read by security software once the person enters a PIN, password, or biometric identifier, providing greater

[5] This might include voice patterns, fingerprints, facial recognition, DNA, palm print, gait analysis, hand geometry, and retinal and iris recognition.

[6] The National Institute of Science and Technology (NIST) created a "Policy for Enabling the Development, Adoption and Use of Biometric Standards" which may be helpful to consult if considering this approach.

security than using a PIN alone, as it requires both physical possession of the smart card and knowledge of the PIN. The PIN, password, or biometric identifier is a secret shared between the person and the microchip device, not between the user and a computer. Microchip devices can be used to further augment the security of a shared secret approach to e-signatures or used in combination with digital signatures.

- **Hybrid, and New Approaches:** Hybrid solutions combine techniques to increase security, authentication, record integrity, and non-repudiation of less secure e-signing methods. A solution might use improved signature-capture techniques combined with click wrap, PINs, and password approaches, while another might use click wrap to encrypt a signature object within read-only document. E-signature solutions requiring high levels of security and non-repudiation might combine the strong authentication of a one-time password token with hashing techniques. Responding to changes in the market, legal, or fiscal environments, new approaches are continually developed. Commercially offered e-signature solutions have matured, with several available that may be compatible with ESRA.

4.2.5 Selecting E-signature Approaches: This is primarily a business decision. Under ESRA, when selecting e-signature approaches for given transactions government entities should support the public's interest in using sound and appropriate practices in governmental e-transactions. While they need not be submitted to ITS for approval, ESRA regulation 9 NYCRR §540.4(c) requires governmental entities to document and maintain a "business analysis and risk assessment" ("BA/RA"), defined in the regulation as: "identifying and evaluating various factors relevant to the selection of an electronic signature for use or acceptance in an electronic transaction. Such factors include, but are not limited to, relationships between parties to an electronic transaction, value of the transaction, risk of intrusion, risk of repudiation of an electronic signature, risk of fraud, functionality and convenience, business necessity and the cost of employing a particular electronic signature process."

The regulatory elements are not a checklist, but rather factors to consider during the BA/RA process. Governmental entities may evaluate each factor differently, accord them different weights based on the specifics of the underlying transaction, and even decide that a particular factor has no weight for a particular transaction. ESRA regulations don't stipulate the extent, level of detail, or format of the required BA/RA. Governmental entities may use their own processes for conducting these assessments, evaluating their specific business needs, risks, and impacts. The regulation also allows governmental entities to collaborate and conduct joint BA/RAs when selecting appropriate e-signature solutions for e-transactions common to such entities. For the same type of e-transaction, they may adopt as their own another governmental entities BA/RA. By combining and leveraging these efforts,

governmental entities, including local governments, can reduce redundant, time-consuming, and costly activities.[7]

4.3 E-Records Guidelines - Background: These are general, technology neutral concepts and guidelines for creating, managing, producing, and maintaining reliable and authentic e-records over time. It describes how governmental entities can protect the authenticity, integrity, security, and accessibility of e-records/e-record systems, but doesn't provide legal advice, explain how to meet e-records statutory or regulatory requirements, nor exclude using other methods of achieving the referenced objectives.

4.3.1 E-Records General Concepts and Guidelines

4.3.1.1 Assessing Legal, Business, and Other Requirements: ESRA defines an "electronic record" as "information, evidencing any act, transaction, occurrence, event, or other activity, produced or stored by electronic means and capable of being accurately reproduced in forms perceptible by human sensory capabilities." This is consistent with definitions of "records" governing legally permissible court admission of, or disposition of, records (NYS Civil Practice Law and Rules §4518; NYS Arts & Cultural Affairs Law Article 57); and the NYS Freedom of Information Law ("FOIL" -- Public Officers Law Art. 6, §86). Creation, format, and management of any types of records are often based on specific factors, so, in considering e-records, governmental entities should consult legal counsel and other appropriate staff to address if their existing recordkeeping practices are based on: required legal mandates; business needs after an e-records system is developed; and past practices managing paper records.

A resource that NYS agencies and local governments (excluding New York City) can use in developing e-record systems is the NYS Archives (NYSA), which provides publications and advisory services concerning records retention, disposition, record management best practices, and, archival requirements equally applicable to e-records as to paper documents. NYC agencies should consult with the NYC Department of Records and Information Services (DORIS) for similar information and guidance.

4.3.1.2 Basing E-records Management Measures on the Records' Value: As with paper, e-records produced or received by governmental entities aren't all of equal importance or value. All government records should be maintained properly, but the effort used by a governmental entity to manage and maintain records, including e-records, should relate to the records' value to the agency and the citizens. Risk management requires deciding what best addresses risk after comparing risks to potential benefits and considering alternate measures to address them. Applying risk management principles to e-records, consider: if e-records were lost or unavailable, how would it impact entity operations, including the entity or others suffering financial loss; the likelihood the e-records would be subject or

[7] As ESRA's named "electronic facilitator" ITS is available to assist governmental entities on completing these assessments, with more detailed guidance as necessary. Contact erecordinglaw@its.ny.gov.

relevant to a legal action; an inability to produce the e-records in admissible form in court having a critical impact on a case's outcome; and, whether the e-records are needed for extended time periods, for business reasons or their significant cultural or historical value.

4.3.1.3 Focusing on E-records Systems and Business Processes: To demonstrate e-record authenticity and integrity, the reliability and accuracy of the systems, processes, and procedures producing and maintaining them are critical, and more important than the format, medium, or technology used. Governmental entities should identify, specify, and document their processes and procedures if they expect their e-records to be accepted in legal and other proceedings.

4.3.1.4 E-records training: Training about systems used to create and retain e-records helps staff adequately maintain and preserve e-record authenticity, integrity, and legal admissibility, and awareness of: the fragile media on which they are stored; technology platforms needed to access and use them; and ensuring their admissibility in legal proceedings, and accessibility throughout their legal retention periods.

4.3.2
Producing E-records:

E-records are created in many ways: internally or using an online application, or received electronically,[8] and must be produced in the required form, with required informational content, unique identifiers, and contextual elements (e.g., authorizations, date stamps, e-signatures). Use precautions in transmitting/receiving e-records to prevent unauthorized persons from tampering with or corrupting them, compromising the e-records' authenticity and integrity. No matter how produced, e-records must be stored in secure recordkeeping systems.

4.3.2.1 Compliance with Legal or Other Requirements:

Document clear procedures for e-record receipt, creation, and storage: Documented policies and procedures should describe acceptable record formats, the point at which a transaction is completed, and specify how the e-record is securely stored so it cannot be modified without detection.

Designate a receiving device: ESRA regulation 9 NYCRR Part 540.5(e) requires governmental entities to designate the receiving "device" where e-records will be accepted, which could mean a specific server, e-mail address, or website. Entities should inform the public of those devices they have designated to receive e-records.

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

[8] The analysis concerning whether electronic attachments to an email constitute electronic records can be exacting. See, for example, Solartech Renewables, LLC v. Vitti, (156 A.D.3d 995 (NY App.Div. Third Dept. 2017)).

4.3.2.2 Authenticating e-Record senders and preventing alteration: To authenticate senders, and determine the integrity of each type of e-record, establish policies and procedures driven by the potential risk and costs if the records were tampered with, inappropriately disclosed, or otherwise proven deficient. Establishing measures to secure e-records and their integrity during transmission and processing will vary with the level of risk, the business requirements, and the technology used. Examples may include: Public Key Cryptography, which provides a very strong encryption for higher risk transactions; Pretty Good Privacy (PGP), a technique for sending secure messages over public networks, or Virtual Private Networks (VPN), used to encapsulate data transfers between devices not on the same private network. Specific techniques may be independently verified or combined to determine if e-records have been altered, including measures as simple as providing the sender with a receipt and copy of the received document, or established data processing techniques such as edit checks, checksum, and hashing techniques, such as those used in digital signature technologies that can detect changes to a record.

Authenticating sender identity based on potential risk and legal requirements: The need for authentication, validating a person's identity, depends on the transaction's nature and business requirements. While some don't require authenticating the sender, if required, there are generally three means to do so, used alone or in combination, concerning something the individual: knows (e.g. a secret, password, PIN, or cryptographic key); possesses (e.g. a token, ATM card or a smart card); or is (e.g. biometric characteristics such as their unique voice pattern or fingerprint). For low to moderate risk applications, typically authentication is done with unique passwords and/or PINs, or unique personal information. Higher risk applications often rely on "two-factor" authentication combining a PIN and something the user "possesses" or "is."

Confirming receipt, and documenting date/time: Some records require confirming document receipt, which varies in relation to the type of application. Web-based applications may return a screen confirming a transaction with a unique tracking/auditing number. High security e-records might confirm separately via alternate routes, e.g. a person's postal address confirmed via an external database and receipt confirmation sent via mail or courier (e.g., FedEx, UPS). Also, some government transactions require documenting date/time receipt information, like a time stamp used on a paper record. This is usually captured automatically by the receiving system, but for high-risk applications, a neutral or trusted third party can apply secure time stamping binding electronic date and time to a record using public key cryptography.

4.3.3 Authentic, Reliable, Accessible E-records Over Time: All e-records must be maintained to be reliable, authentic, accessible, and usable for their legal retention periods. Those with long term or permanent retention requirements must be preserved in accessible and usable form or, for NYS agencies, transferred to NYSA. Other

governmental entity e-records should be legally destroyed only under a records disposition authorization issued by NYSA or, for NYC, DORIS.

4.3.3.1 E-records Management Policies: Policies should:

- **Specify what e-records are covered:** Group e-records into "types" or "series" manageable in a consistent manner, e.g. by the business activity that created them ("vehicle registration," "fishing license file"), or to generic group ("accounting data," "customer documents"). E-records more critical for entity operations or more likely needed for legal purposes should have more management attention and higher levels of protection. NYSA retention and disposition schedules provide guidance in determining record series for governmental e-records.

- **Establish file format standards**: Designate approved data file formats for each record "type." Retrieving and displaying information on computer systems requires software which can change, either through new releases, or by changes to operating systems or hardware. A policy of approved media formats for e-records storage will facilitate data migration to ensure long-term retrieval of e-records.

- **Define responsibilities:** Define responsibilities for implementing the policy among program and technical staff, and those specifically assigned to records management.

- **Develop controlled storage or filing systems maintaining e-record integrity and accessibility:** Once created or captured, e-records must be retained in controlled environments maintaining their integrity and authenticity, in secure, reliable, and trustworthy e-records systems detecting and preventing unauthorized modifications. Document management or knowledge management products provide such solutions. The U.S. Department of Defense also tests and certifies document management products that include e-records management capabilities.

4.3.3.2 Retain E-records Accessibly for their Legal Minimum Retention Periods:

Use law-compliant records retention and disposition schedules: Records retention and disposition schedules address general functions of NYS agencies and non-NYC local governments, but consulting NYSA's website and following NYSA's procedures, can develop schedules for unique records, including e-records.[9]

Plan for covering data backup, disaster recovery, and emergency operations: Contingency plans helping governmental entities quickly restore systems after a disaster should include data backup and recovery to prevent loss of e-records.

[9] NYC agencies should contact NYC's DORIS.

Implement media controls: Physical and environmental threats can impact e-records, especially those stored on fragile data storage devices. Provide control over the many forms of physical data storage through standard labeling and tracking log practices and ensuring backup data storage devices are stored in environmentally and physically controlled locations. The extent of media control depends on the type of data, quantity of media, and the nature of the user environment. Media storing critical or high-risk e-records will normally demand higher levels of control than other data.[10]

Perform routine backups: Software and data including e-records require backups, whose frequency depends on how often data changes and the importance of the changes. Consult program managers to determine appropriate backup schedules. Externally securely store and test backup copies to ensure they remain usable.

Make e-records retrievable during their retention periods but destroyed thereafter: Use adequate indexing and search tools allowing retrieval when e-records are stored on nearline or physical data storage devices. But e-records having met their legal retention requirements and serving no other business needs should be destroyed. Destruction involves controlling all copies on all computers, detachable equipment, and media; documenting destruction; and using appropriate media sanitization and destruction methods depending on the e-records' confidentiality.[11]

4.3.3.3 Producing authentic e-record copies in usable formats

Ensure e-records are included in personal privacy protection/access policies: Maintain consistency with NYS FOIL, Personal Privacy Protection Law (PPPL), agency specific laws, and ESRA. NYS agency websites must comply with the Internet Security and Privacy Act (NYS Technology Law, Article II), adopting and posting an Internet privacy policy describing management, retention, and disclosure of users' personal information. ITS provides NYS agencies a model policy with items to take into account.

E-records public access methods must protect confidentiality: Governmental e-record systems must balance the need for e-records' public access against the entity's duty to protect confidentiality. Consider using automated means to redact or mask confidential information from e-records before releasing them to the public.

E-record access in the user's preferred form: Some lack access to technology for using e-records, while others prefer paper records. Per ESRA and its

[10] Academic institutions including Cornell and M.I.T. publish, available from their libraries, tutorials concerning "Digital Preservation Management."

[11] ITS policies, and NIST Special Publication 800-88 Rev. 1, "Guidelines for Media Sanitization," have detailed recommendations on the sanitization and destruction of most types of digital media.

regulations[12] while maintaining paper copies of e-records isn't required, governmental entities must generate legible and usable paper copies if requested.

4.3.3.4 Maintaining the Authenticity/Integrity of Electronically Signed E-records: Not all e-records are e-signed, but those that are require preserving the context and links between components. Such contextual information provides additional evidence supporting the reliability and authenticity of the signed e-record and/or may actually constitute the e-signature process itself. Key challenges governmental entities face in maintaining electronically signed e-records include determining what information must be retained to maintain a valid, authentic, and reliable signed e-record, and preserving the link or association between the various components of a signed record over time.

Determining the minimal information needed to prove authenticity and reliability of an electronically signed record in a legal proceeding requires a legal analysis.[13] When preparing their e-signature BA/RAs and deciding what information needs to be retained as part of the signed e-record, governmental entities should research caselaw for decisions about challenges to the authenticity or validity of an e-signature, or assessing the reliability of an e-signed record on the basis of its e-signature. The e-signature method selected will partially determine the approaches needed to ensure the trustworthiness of the e-signed e-record over time. In "Guidance on Managing Digital Identity Authentication Records," the National Archives and Records Administration (NARA) has identified practices used by Federal agencies, including: maintaining adequate documentation of an e-signature's validity gathered at or near the time the e-record was signed, where, depending on the signing method, this contextual information may actually be part of the signed e-record or captured in supporting records; or maintaining the ability to revalidate e-signatures (requiring agencies to retain the capability to revalidate the e-signature, along with retaining the signed e-record). As with any e-record, acceptance of signed e-records for legal, audit, and other purposes depends on demonstrating the trustworthiness of the system used to produce them, and, maintaining the ability to revalidate e-signatures is only available where the e-signature method relies primarily on a digital object that can be revalidated (e.g., an encrypted hash, a digitized signature, or a biometric). Retaining all records of the system's functionality specific to a particular e-signature technology or approach is needed for the revalidation process to be successful. For digital signatures produced with PKI, ensure the PKI is governed by a certificate policy addressing all aspects of a digital certificate's generation, management, use, and storage as well as the roles and responsibilities of all entities involved in the PKI. And, regardless of approach used, retain documentation of the signer's identity; how, and the

[12] 9 NYCRR Part 540.5(b)(1)

[13] Some court decisions addressing the proper evidentiary foundation that should be established when e-documents are submitted for admission into evidence, while not controlling, are informative on this topic, such as: In re: Vee Vinhnee, 336 B.R. 437, (9th Cir. BAP (Cal.) Dec 16, 2005); and Lorraine v. Markel American Insurance Company, 241 F.R.D. 534 (D. Md. 2007).

date/time, they were authenticated; signer's intent; and date/time the signing process was completed.

Preserve links between signed e-records components over time: Systems creating e-records should manage all signed e-record components, even revalidating an e-signature where possible. Lacking relatively short retention need, records may be migrated to a new system or ultimately stored offline. Retaining contextual information is crucial for signed e-records, and plans should address signed e-record retention requirements, so those with longer retention periods (6 years+) can be migrated to new systems or stored on data storage devices while preserving the link and associations of their various components. If the e-record creating system's functionality is no longer available, preserving the relationship of the various components of the signed e-record may involve reformatting it., in a planned, well documented, conducted-in-the-normal- course-of-business process, in a way the records' authenticity, integrity, and reliability can be shown. Seriously consider if the ability to revalidate an e-signature throughout a signed e-records retention period is really critical. Retaining an ability to revalidate an e-signature may be a difficult and costly task especially for records with longer retention periods, requiring use of long-term signature validation services.[14]

Maintaining adequate documentation of an e-signature's validity, and ability to re-validate an e-signature at a later date, are not necessarily mutually exclusive options. Both strategies can be used simultaneously or during different stages in the e-record's life cycle. Base using these options on business requirements and assessment of risks, determining how long an e-signature needs to be validated, and if something other than original signature validation is acceptable. The ability to document and revalidate a signature could be maintained during periods of highest risk of repudiation, or during the record's active life. During its inactive storage, with lower repudiation risk, an entity may determine it can rely solely on documentation about the signed e-record's validity.[15]

5.0 Compliance

This guideline shall take effect upon publication. Compliance with enterprise guidelines is optional, but strongly suggested. ITS may amend its guidelines at any time; compliance with amended guidelines is optional, but strongly suggested.

[14] Note that for PKI-supported digital signatures, lengthy e-records retention requirements may outlive any agreement with, or even existence of, the CA. Long-term signature validation services must be viewed as a separate function that cannot be left solely to an independent CA.

[15] NARA is one organization with record management and retention "Transfer Guidance" for digital signature authentication. Governmental entities could also review guidance issued by the National Archives of Canada, and the Australian National Archives, which generally question the practicality of maintaining ability to revalidate signed e-records maintained for long time periods or permanently, and suggest maintaining adequate documentation of validity gathered at or near the time of record signing instead may be preferable for such e-records. Such an approach is less dependent on technology, and much more easily maintained as technology evolves over time.

6.0 Definitions of Key Terms

Except for terms defined in these ESRA Guidelines, or in the ESRA statute and regulations, all terms shall have the meanings found in https://www.its.ny.gov/glossary.

7.0 Contact Information

Submit all inquiries and requests for future enhancements to the policy owner at:

Division of Legal Affairs
Reference: NYS-G04-001
NYS Office of Information Technology Services
State Capitol, PO Box 2062
Albany, NY 12220-0062
Telephone: (518) 473-5115
Email: its.sm.dla@its.ny.gov

Statewide technology policies, standards, and guidelines may be found at the following website: https://its.ny.gov/tables/technologypolicyindex

8.0 Revision History

This guideline shall be reviewed at least once every year to ensure relevancy.

Date	Description of Change	Reviewer
05/26/2004	Original ESRA Guidelines issued.	CIO/OFT
09/28/2007	Revised and republished.	CIO/OFT
10/23/2007	Reformatted and updated to reflect current CIO, agency name, logo and style.	CIO/OFT
11/02/2011	Revised and republished.	CIO/OFT
12/20/2013	Revised and republished.	ITS
09/6/2017	Revised and republished.	ITS
05/04/2021	Revised and republished. Reformatted and updated in entirety.	Division of Legal Affairs

9.0 Related Documents

NYS Resources:

- Unofficial copies of ESRA law and regulations: https://its.ny.gov/electronic-signatures-and-records-act-esra

- NYS IT Policy P10-006 - "Identity Assurance" (NYS Identity Trust Model. https://its.ny.gov/tables/technologypolicyindex

- NYSA publications relevant to e-signatures and e-records include: Digital Imaging Guidelines; Conducting Needs Assessments for New Recordkeeping Systems (Tech. Information Series #64); Preparing for the Worst: Managing Records Disasters (Tech. Information Series #82); Managing Voice Mail Records; Developing a Policy for Managing email (Tech. Information Series #85); Managing email Records; Guidelines for Choosing Records Management Software (Tech. Information Series #63); Indexing Records; and Managing Geographic Information Systems (GIS) Records. http://www.archives.nysed.gov/publications.

- NYS-DOS Committee on Open Government's website has NYS FOIL law complete text, and FAQs/advisory opinions addressing e-records issues: https://www.dos.ny.gov/coog/

- NYS Unified Court System Office of Records Management publications: http://ww2.nycourts.gov/admin/recordsmanagement/too_pubstrain.shtml

- University at Albany's Center for Technology in Government e-signatures and e-records-related publications, including: Building State Government Digital Preservation Partnerships: A Capability Assessment and Planning Toolkit, Version 1.0; Opening Gateways: A Practical Guide for Designing Information Access Programs; Practical Tools for Electronic Records Management and Preservation; The Records Requirements Analysis and Implementation Tool; Preserving State Government Digital Information: A Baseline Report; Building State Government Digital Preservation Partnerships; Exemplary Practices in Electronic Records and Information Access Programs; Models for Action: Practical Approaches to Electronic Records Management & Preservation; Functional Requirements to Ensure the Creation, Maintenance, and Preservation of Electronic Records; A Survey of Key Concepts and Issues for Electronic Recordkeeping; and A Framework for Evaluating Public Sector Geographic Information Systems. See: https://www.ctg.albany.edu/publications/

Other Resources

- Cornell University/MIT tutorial, "Digital Preservation Management: Implementing Short-Term Strategies for Long Term Problems."

- Council on Library and Information Resources (CLIR) publications, "The State of Digital Preservation: An International Perspective" and "Authenticity in a Digital Environment" covering digital preservation research, development, and technical approaches, and "Magnetic Tape Storage and Handling."

- Joint Interoperability Test Command, DISA, DoD, Records Management Application publications.

- NIST Computer Security Special Publications, providing standards and guidelines re: digital signatures, PKI, system security, and risk management.

- National Archives of Australia provides a number of guidelines and publications on managing and preserving e-records.

- NARA publication, "Records Management Guidance for Agencies Implementing Electronic Signature Technologies."

- Office of Management and Budget (OMB): "OMB Circular No. A-130:
- "Managing Information as a Strategic Resource".

- Property Records Industry Association (PRIA), non-technical documents concerning e-recording real property instruments: "How to Get Ready for eRecording – Recorders" and "How to Get Ready for eRecording – Submitters." ITS expressly incorporated by reference into ESRA regulations the "PRIA Guidelines" available via the PRIA website.

- Some e-signature technologies are based on cryptographic techniques (e.g. PKI). Concerning their security, see federal government technical standards and guidelines such as: FIPS 140-2, "Security Requirements for Cryptographic Modules," and NIST's "Introduction to Information *Security.*"