



MANUAL TRANSMITTAL

Department of the Treasury
Internal Revenue Service

10.10.1

AUGUST 12, 2024

EFFECTIVE DATE

(08-12-2024)

PURPOSE

- (1) This transmits revised IRM 10.10.1, Identity Assurance, IRS Electronic Signature (e-Signature) Program.

MATERIAL CHANGES

- (1) IRM 10.10.1.3.1.5, Preserving the Integrity of the Signed Electronic Record- Added IRM reference for additional guidance on electronic records.
- (2) IRM 10.10.1.4, Secure Storage- Removed outdated paragraph about storage systems requiring indexed retrieval systems and reproducing hard copies.
- (3) IRM 10.10.1.6, Deviating from the e-Signature Policy Requirement- Moved “Note” from IRM 10.10.1.6.3 to clarify the subsections the guidance applies to. Added reference to IRM 10.10.1.6.3 to capture the subsection as an applicable scenario for a deviation.
- (4) IRM 10.10.1.6.1, Accepting Images of Signatures and Digital Signatures in Certain Taxpayer Interactions- Updated to clarify the interactions and employees this guidance applies to.
- (5) IRM 10.10.1.6.3, Accepting Provisional Signatures on Other Forms- Moved “Note” to IRM 10.10.1.6 to clarify its applicability to nested subsections.
- (6) Exhibit 10.10.1-1, Current Approved Methods- Added Form 1042, Annual Withholding Tax Statement for U.S. Source Income of Foreign Persons to capture e-File capability.
- (7) Exhibit 10.10.1-2, Deviation from Handwritten Signature requirement for Limited List of Tax Forms Memorandum - Added Form 3911, Taxpayer Statement Regarding Refund. Removed Form 1042, Annual Withholding Tax Statement for U.S. Source Income of Foreign Persons.
- (8) Throughout, made editorial changes for clarity. Reviewed and updated grammar, website links, plain language and IRM references.

EFFECT ON OTHER DOCUMENTS

None

AUDIENCE

The intended audience is IRS employees who determine policy, and/or receive electronic documents or digital transactions with e-Signatures.

Angela R. Gartland
Director, Identity Assurance Office

10.10.1

IRS Electronic Signature (e-Signature) Program

Table of Contents

10.10.1.1 Program Scope and Objectives

10.10.1.1.1 Background

10.10.1.1.2 Authority

10.10.1.1.3 Roles and Responsibilities

10.10.1.1.4 Program Management and Review

10.10.1.1.5 Terms and Acronyms

10.10.1.1.6 Related Resources

10.10.1.2 Introduction to IRS e-Signature Policy

10.10.1.3 Electronic Signatures

10.10.1.3.1 Requirements for Legally Binding Electronic Signatures

10.10.1.3.1.1 Acceptable Forms of Electronic Signatures

10.10.1.3.1.2 Intent to Sign the Electronic Record

10.10.1.3.1.2.1 Confirming Intent to Sign the Electronic Record

10.10.1.3.1.3 Attachment or Association of the Electronic Signature with the Electronic Record

10.10.1.3.1.3.1 Embedding or Associating the Integrity of the Signature

10.10.1.3.1.4 Identifying and Authenticating the Signer

10.10.1.3.1.5 Preserving the Integrity of the Signed Electronic Record

10.10.1.4 Secure Storage

10.10.1.5 Complying with the e-Signature Policy Requirements

10.10.1.6 Deviating from the e-Signature Policy Requirements

10.10.1.6.1 Accepting Images of Signatures and Digital Signatures in Certain Taxpayer Interactions

10.10.1.6.2 Accepting Electronic or Digital Signatures in lieu of Handwritten Signatures for Limited List of Tax Forms

10.10.1.6.3 Accepting Provisional Signatures on Other Forms

10.10.1.7 Oversight Procedure

Exhibits

10.10.1-1 Current Approved Methods

10.10.1-2 Deviation from Handwritten Signature Requirement for Limited List of Tax Forms Memorandum

10.10.1-3 Glossary and Acronyms

10.10.1.1
(10-17-2023)
Program Scope and Objectives

- (1) **Purpose:** This IRM covers Servicewide e-Signature policies and procedures, including:
- Defining e-Signature terms and IRS e-Signature principles.
 - Establishing minimum baseline requirements for taxpayer e-Signatures that are required on forms, documents and web applications.
 - Adopting an e-Signature signing process.
 - Ensuring all e-Signatures have the appropriate risk and authentication requirements in place to ensure compliance with relevant federal government policies.
 - Providing business and form owners a resource regarding e-Signature solutions and for complying with e-Signature policy.
 - Assigning roles and responsibilities for all key stakeholders to implement e-Signature solutions, identify and mitigate risks, and ensure compliance with e-Signature requirements.
 - Performing oversight functions and compliance functions within the e-Signature program.

Note: This IRM does not address the following:

Electronic signature requirements for internal use IRS documents.

Taxpayer signatures received through Enterprise Electronic Fax (EEFax).

- (2) **Audience:** The intended audience is IRS employees who determine policy, and/or receive electronic documents or digital transactions with e-Signatures.
- (3) **Policy Owner:** The director of Identity Assurance (IA), under Privacy, Governmental Liaison and Disclosure (PGLD).
- (4) **Program Owner:** IA within PGLD is the program office responsible for providing e-Signature guidance and support. Each business unit is responsible for applying the guidelines in this IRM.
- (5) **Primary Stakeholder:** All organizations and business units who receive taxpayer documentation electronically that include e-Signatures.
- (6) **Program Goals:** The goal of this IRM is to define uniform standards for the acceptance of taxpayer signatures appearing in electronic form and ensure compliance with federal requirements and policies.
- (7) **Contact Information:** To recommend changes or make any other suggestions to this IRM section, email the IA office at **PGLD IA eSignature*.

10.10.1.1.1
(10-17-2023)
Background

- (1) Electronic signatures are governed by laws and guidance specified in IRM 10.10.1.1.2, Authority.

10.10.1.1.2
(10-17-2023)
Authority

- (1) IRC 6061, directs the Secretary of the Treasury to “develop procedures for the acceptance of signatures in digital or other electronic form.” This IRM establishes those procedures.
- (2) The IRS’s e-Signature policy implements relevant authentication laws, mandates, and compliance policies.
- (3) For reference, other electronic signature laws include those in the list below. The goal of these e-Signature laws is to specify criteria which, once met by an electronic signature, enable such electronic signature to enjoy the same level

of legal recognition as a corresponding handwritten signature. They do not supersede or take priority over IRC 6061 , which specifically addresses the signing of returns and other documents required under internal revenue tax laws and regulations.

- a. **Electronic Signatures in Global and National Commerce Act (E-SIGN)** - a federal law enacted in 2000 that largely preempts inconsistent state law (although in certain cases state law may still control) and that is applicable to commercial, consumer, or business transactions involving federal organizations.
- b. **Uniform Electronic Transactions Act (UETA)** - a uniform state law that was finalized by the National Conference of Commissioners on Uniform State Laws (NCCUSL) in 1999 and subsequently adopted by 49 states, and which may be applicable to commercial, consumer, or governmental affairs transactions involving federal organizations in certain cases.
- c. Other federal government guidelines on electronic signatures include:
 - **Government Paperwork Elimination Act (GPEA)** - a federal law enacted in 1998 that is applicable to governmental transactions and other transactions involving certain federal organizations.
 - **National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 (Rev. 5), Appendix C** - outlines security and privacy controls designed within an effective risk management framework, to implement fundamental safeguards and countermeasures necessary to protect information during processing, while in storage, and during transmission.
 - **NIST Digital Identity Guidelines (SP 800-63-3)** - applies to all federal agencies implementing digital identity services. NIST SP 800-63-3 guidance outlines technical ID Proofing and authentication requirements. The separation into categories provides agencies flexibility in choosing identity solutions and increases the ability to include privacy-enhancing techniques as fundamental elements of identity systems at any assurance level.
 - **Office of Management and Budget (OMB) Memorandum (M) 19-17**, Enabling Mission Delivery through Improved Identity, Credential and Access Management or successor documents.
 - **Use of Electronic Signatures in Federal Organizations Transactions (UESFOT)**, Version 1.0 issued January 25, 2013.
 - **Public Law No: 115-336, 21st Century Integrated Digital Experience Act**, enacted on December 20, 2018, that requires executive agencies to submit a “plan to accelerate the use of electronic signature standards established under the Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001 et seq).”

10.10.1.1.3 (10-17-2023)

Roles and Responsibilities

- (1) IA's role is to strengthen the IRS authentication posture by enhancing visibility and coordination for:
 - Identity proofing
 - Authentication
 - Authorization
 - Access strategies, processes controls and capabilities
- (2) IA assists in ensuring that an electronic signature complies with federal laws and regulations.

- (3) The director of IA is responsible for the e-Signature policy guidance.
- (4) Organization executives and management officials who lead programs described in this policy are responsible for these guidelines, specifically to ensure that electronic signatures conform to the policy in this IRM.
- (5) Each IRS organization is responsible for establishing internal processes for implementing e-Signature solutions based upon this guidance.
- (6) IA provides e-Signature policy guidance and subject matter expertise on both procedural issues and complex legal issues. Before seeking our assistance, you as the form or transaction owner needs to consult with Counsel to determine if an electronic signature can be used on your form.
- (7) IA is responsible for the e-Signature policy. To meet this responsibility, IA personnel must be kept informed of the problems and questions that the IRS functions encounter regarding e-Signature.

10.10.1.1.4
(10-17-2023)
**Program Management
and Review**

- (1) IA works closely with business units to ensure that the requirements of this IRM are reflected in e-Signature technical planning, capability development, and implementations. Additional control information can be found in the business unit IRM where the program/procedure resides.

10.10.1.1.5
(10-17-2023)
Terms and Acronyms

- (1) Exhibit 10.10.1-3, Glossary and Acronyms contains a table of terms, acronyms, and definitions.

10.10.1.1.6
(12-03-2019)
Related Resources

- (1) IRC 6061(b)
- (2) 26 CFR 301.6061-1
- (3) IRM 10.5.1, Privacy Policy

10.10.1.2
(10-17-2023)
**Introduction to IRS
e-Signature Policy**

- (1) IRS modernization efforts to enable digital transactions includes expanding e-Signature capabilities. Increasing digitalization will streamline processes, improve access to digital data and lessen the IRS's environmental impact. A form or transaction needs to be digitized before the IRS can collect an e-Signature.
- (2) The IRS e-Signature principles and federally mandated authentication controls describe how the IRS protects an individual's identity and assures that only authorized signers are completing the transaction.
- (3) Adherence to IRS e-Signature principles and requirements is mandatory to preserve the integrity of the signed IRS record.
- (4) IRS e-Signature requirements form the basis for implementing technology and security controls.
- (5) This IRM provides a framework for applying e-Signature consistently across the IRS. It will guide how the IRS executes electronic transactions and will be an essential component of an IRS online authorization capability.

10.10.1.3
(10-17-2023)
Electronic Signatures

- (1) “Electronic signature” is the term used in all E-transaction laws for the electronic equivalent of a handwritten signature. It is a generic, technology neutral term that refers to the universe of all the various methods by which one can “sign” an electronic record.
- (2) A compliant IRS electronic signature is one which meets the core requirements outlined in IRM 10.10.1.3.1, Requirements for Legally Binding Electronic Signatures.
- (3) See IRM 10.10.1.6, Deviating from the e-Signature Policy Requirement for alternative methods to sign an IRS document electronically.

10.10.1.3.1
(12-03-2019)
Requirements for Legally Binding Electronic Signatures

- (1) Each permitted electronic signing process must satisfy each of the following five requirements:
 - a. The signer(s) must use an acceptable form of electronic signature(s) described in IRM 10.10.1.3.1.1, Acceptable Forms of Electronic Signatures.
 - b. The electronic signature(s) must be executed or adopted by a person(s) in a manner that meets IRM 10.10.1.3.1.2, Intent to Sign the Electronic Record, that demonstrates the intent of the person(s) to sign the electronic record.
 - c. The electronic signature(s) must be attached to or associated with the electronic record being signed in accordance with IRM 10.10.1.3.1.3, Attachment or Association of the Electronic Signature with the Electronic Record.
 - d. There is a means to identify and authenticate a person(s) as the signer(s) in accordance with IRM 10.10.1.3.1.4, Identifying and Authenticating the Signer, and the signer must be authorized to execute the document.
 - e. There is a means to preserve the integrity of the signed electronic record in accordance with IRM 10.10.1.3.1.5, Preserving the Integrity of the Signed Electronic Record.

10.10.1.3.1.1
(10-17-2023)
Acceptable Forms of Electronic Signatures

- (1) Electronic signatures can take many forms and can be created by many different technologies. No specific technology or form of signature is required.
- (2) Any electronic sound, symbol, or process can be used as the form of electronic signature provided the form of electronic signature is permitted for use on the specific IRS document by IRS guidance.
- (3) If permitted by IRS guidance on the specific IRS document, the following forms of electronic signature are currently permissible for use:
 - a. A typed name that is typed within or at the end of an electronic record, such as typed into a signature block.
 - b. A scanned or digitized image of a handwritten signature that is attached to an electronic record.
 - c. A shared secret, such as a code, password, or Personal Identification Number (PIN).
 - d. A unique biometric-based identifier, such as a fingerprint, voice print, or a retinal scan.
 - e. A handwritten signature input onto an electronic signature pad.
 - f. A handwritten signature, mark, or command input on a display screen by means of a stylus device.

- g. A selected checkbox on an electronic device such as a computer or tablet.
- h. A signature created by a third party software.

Note: See Exhibit 10.10.1-1, Current Approved Methods, for a listing of approved signature methods and their related forms.

10.10.1.3.1.2
(10-17-2023)

Intent to Sign the Electronic Record

- (1) An electronic signature must be executed or adopted by the signer with the intent to sign the electronic record.
- (2) Intent to sign can be inferred from a signer's approval of the reason for signing the electronic record as stated in the text of the record being signed or elsewhere in the signing process.

10.10.1.3.1.2.1
(10-17-2023)

Confirming Intent to Sign the Electronic Record

- (1) Each permitted electronic signing process will require that the context in which an electronic signature is applied or the process by which a person applies an electronic signature to the record includes a step where the signer confirms intent to sign the record.
- (2) The signer must establish the intent to sign through a clear and conspicuous notice that a document is being signed with an electronic signature. The notice must include:
 - a. A description of the signing process.
 - b. A clear statement of the purpose for the electronic signature.
 - c. A statement that the completed signing process will constitute the signer's legally binding signature.
- (3) The purpose for signing with an electronic signature must be described in the text of the document being signed.
- (4) The signer may confirm intent to sign by either of these methods:
 - a. Requesting confirmation of the signer's electronic signature whereby the signer must acknowledge the signer's electronic signature and then providing the option to cancel, or
 - b. Continuing, or adding a submission step following the signature step whereby the signed records are not effective until submitted.
- (5) Each permitted electronic signing process must include requirements that minimize the risk that signers could:
 - a. Disavow their electronic signature.
 - b. Claim they did not understand the legal significance of the electronic signature.
 - c. Claim they did not understand the reason for signing.
 - d. Claim they did not intend to sign.

10.10.1.3.1.3
(10-17-2023)

Attachment or Association of the Electronic Signature with the Electronic Record

- (1) The electronic signature must be attached to or associated with the electronic record in a manner that establishes that an electronic signature was applied to a specific electronic record. The signing process must:
 - a. Apply the electronic signature to a document that the signer can perceive and review in a manner that makes clear to the signer exactly what is being signed.

- b. Attach or associate the electronic signature to the electronic record by linking the electronic signature and making it a part of the electronic record being signed.

- (2) The permitted electronic signing process must be clear so that the signer knows exactly what IRS document is being signed.

10.10.1.3.1.3.1
(10-17-2023)
**Embedding or
Associating the Integrity
of the Signature**

- (1) Each permitted electronic signing process will require that the electronic signature be associated with the electronic record being signed. After the electronic record has been signed, the electronic record must be tamper-proof to ensure that the signature(s) applied to or associated with one record is not applied to or associated with another record and to prevent the contents of the record to which the signature(s) applied from being altered.
- (2) Alternatively, the permitted electronic signing process will require the data representing the electronic signature to be stored separately from the electronic record being signed, provided a demonstrably reliable and provable process is in place which will include a relational database or a digital signature algorithm to associate the electronic signature with the electronic record.

10.10.1.3.1.4
(10-17-2023)
**Identifying and
Authenticating the
Signer**

- (1) The electronic signing process must identify and authenticate a person as the signer and source of the electronic document or message.
- (2) The electronic signing process must be able to generate evidence of the person to whom the electronic signature belongs and generate evidence that the identified person is associated with the electronic record.
- (3) The procedures for authenticating the signer for any specific digital transaction or form depends on a risk assessment outlined in IRM 10.10.1.7, Oversight Procedure.
- (4) If there is more than one signer required for the electronic record, the electronic signing process must be designed to separately identify and authenticate each signer.

10.10.1.3.1.5
(10-17-2023)
**Preserving the Integrity
of the Signed Electronic
Record**

- (1) Electronic signatures must be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record.
- (2) After the electronic record has been signed, the electronic record must be tamper-proof to ensure that the signature(s) applied to or associated with one document is not applied to or associated with another document and to prevent the contents of the document to which the signature(s) applied from being altered. For additional guidance on electronic records, see IRM 1.15.6, Managing Electronic Records.

10.10.1.4
(08-12-2024)
Secure Storage

- (1) Each electronic signing process permitted for use on a specific IRS document by IRS guidance will require that the data constituting the electronic signature be stored in a manner that permanently attaches or associates the electronic signature with the electronic record that was signed.
- (2) An electronic signature created using a set of actions, steps, and elements, requires the generation of a specific data element that indicates completion of

the electronic signing process. The data element or procedure must be permanently attached to or associated with the electronic record that was signed.

- (3) Each permitted electronic signing process requires techniques to lock the electronic record and prevent it from being modified.
- (4) Storage systems require secure access control to ensure that the electronic records cannot be modified.

Note: See IRM 1.15.6.5, Creation, Use, and Maintenance of Structured Electronic Data, for guidance on ensuring electronic information systems that produce, use, or store data have disposition instructions incorporated into the system design. The National Archives and Records Administration (NARA) is responsible for issuing standards for management of federal records created or received on electronic systems.

- (5) All IRS employees and contractors are responsible for ensuring IRS records (hard copy and electronic) are appropriately managed, retained, and archived in accordance with IRM 1.15, Records and Information Management, on records retention and disposition requirements before documents can be destroyed. The electronic records retention period includes the period by which the record may be material for tax administration purposes. Refer to Document 12990, IRS Records Control Schedules (RCS), for the NARA-approved IRS records disposition to prevent unauthorized/unlawful destruction of records. Refer to Document 12829, General Records Schedules (GRS), for the NARA-issued disposal authorizations for temporary administrative records common to all Federal agencies. The IRS has issued guidance to taxpayers that maintain books and records using an electronic storage system, including guidance on when these records will constitute records within the meaning of IRC 6001. See Rev. Proc. 97-22 , 1997-1 C. B. 652 (Guidelines for Electronic Storage of Documents by Taxpayers).

Note: On January 10, 2023, Rev. Proc. 97-22 was posted in the Federal Register for comment and eventual update. No changes are made to the Revenue Procedure at this time.

10.10.1.5 (10-17-2023) Complying with the e-Signature Policy Requirements

- (1) IA provides consultation, best practices and subject matter expertise. Business operating division and functional operating division (BOD/FOD) owners and form owners are responsible for implementing an e-Signature.
- (2) IA facilitates conversations between parties, (e.g., BOD/FOD owners and IT) providing Authentication, Authorization, and Access (A3) compliance knowledge and ensuring all appropriate stakeholders participate to identify and implement the e-Signature policy based on the form owners requirements.
- (3) BOD/FOD owners/form owners who require subject matter expertise on the e-Signature process should contact IA through the e-Signature mailbox, **PGLD IA eSignature*, to request assistance.
- (4) If the BOD/FOD owner is unable to meet the requirements stated in IRM 10.10.1, Identity Assurance, IRS Electronic Signature (e-Signature) Program, to comply with the e-Signature policy, they may explore a deviation from the e-Signature requirements. A request must be sent to the e-Signature mailbox **PGLD IA eSignature*. Once supported or approved, the deviation will remain in

place until the forms meet the requirements stated in IRM 10.10.1.3.1, Requirements for Legally Binding Electronic Signatures.

10.10.1.6
(08-12-2024)
**Deviating from the
e-Signature Policy
Requirements**

- (1) The IRS will accept e-Signatures that do not meet the requirements listed in IRM 10.10.1.3.1 if they apply to the scenarios described in IRM 10.10.1.6.1, Accepting Images of Signatures and Digital Signatures in Certain Taxpayer Interactions IRM 10.10.1.6.2, Accepting Electronic or Digital Signatures in lieu of Handwritten Signatures for Limited List of Tax Forms and IRM 10.10.1.6.3, Accepting Provisional Signatures on Other Forms.

Caution: The e-Signature deviations permitted in this subsection do not establish a precedent for acceptable use of these e-Signatures in other circumstances.

Note: Once the option to file these forms electronically, or to accept e-Signatures that meet the requirements in IRM 10.10.1.3.1, Requirements for Legally Binding Electronic Signature, is available, the deviations will no longer be allowed.

10.10.1.6.1
(08-12-2024)
**Accepting Images of
Signatures and Digital
Signatures in Certain
Taxpayer Interactions**

- (1) Applicable taxpayer interactions include the following:
 - a. Authenticated, recurring interactions of IRS personnel working person-to-person with taxpayers to address or resolve issues (e.g., field compliance, Appeals, Counsel, and Taxpayer Advocate Service personnel).
 - b. Campus compliance cases worked in response to a solicitation from the IRS (e.g., campus exam, automated underreporter, and campus collection).
- (2) Employees may accept images of signatures and digital signatures on documents related to the determination or collection of a tax liability or to the settlement of tax controversies.
- (3) This applies to any statement or form traditionally exchanged between IRS personnel and taxpayers during these taxpayer interactions outside of standard filing procedures.

Caution: Tax returns must be filed in accordance with the instructions for the respective form.

- (4) Before accepting a document with an electronic signature from a taxpayer:
 - a. Employees working person-to-person must authenticate the taxpayer or representative by phone or in-person to ensure they are authorized to sign the document in question. See IRM 11.3.2.3.2, Requirements for Verbal or Electronic Requests.
 - b. Employees working campus compliance cases must ensure the document is the result of a solicitation from the IRS (e.g., response to a letter or notice mailed to the taxpayer).
- (5) The following are acceptable signatures:
 - a. Images of documents with original signatures (scanned or photographed) in any common file type such as JPEG, TIFF, PDF, etc.

- b. Digital signatures that use encryption techniques that provide proof of original and unmodified documentation when transmitted by an approved secure messaging or file transfer system.

Note: Transmission and receipt of these forms are subject to IRS procedures. Refer to IRM 10.5.1.6.8, Email and Other Electronic Communications, and IRM 10.5.1.6.9, Other Forms of Transmission.

Note: The IRS has a *secure online platform* for submitting certain forms. Taxpayers are encouraged to make as much use of this platform as possible.

10.10.1.6.2
(11-18-2021)
Accepting Electronic or Digital Signatures in lieu of Handwritten Signatures for Limited List of Tax Forms

- (1) Taxpayers and representatives may use electronic or digital signatures when signing certain forms that currently require a handwritten signature and that cannot be filed using IRS e-File.
- (2) See Exhibit 10.10.1-2, for a list of forms where such electronic or digital signatures are permitted.

10.10.1.6.3
(10-17-2023)
Accepting Provisional Signatures on Other Forms

- (1) Form or transaction owners may request temporary deviations from the signature requirements described in IRM 10.10.1.3.1, Requirements for Legally Binding Electronic Signatures.
- (2) IA together with the form or transaction owner, may conduct a risk assessment to determine if a 'non-compliant' electronic signature is possible. The identified risks, mitigations and decisions must be documented in a Form 14675, Decision Making Framework Risk Acceptance Form and Tool (RAFT).
- (3) Form or transaction owners will be responsible for completing e-Signature risk assessments.
- (4) Any IRS document that is signed using the permitted electronic signing process will be treated for all purposes (both civil and criminal, including penalties for perjury) in the same manner as though signed with a handwritten signature. See IRM 10.10.1.7, Oversight Procedure.

10.10.1.7
(10-17-2023)
Oversight Procedure

- (1) The IRS requires all electronic customer facing applications that require authentication to complete a risk assessment process.
- (2) e-Signatures are electronic transactions by definition and require a risk assessment.
- (3) The IRS uses the Digital Identity Risk Assessment (DIRA) framework to assess risks associated with electronic transactions.
- (4) IA together with the business owner will use the DIRA to determine the appropriate identity proofing and authentication protocol in addition to completing an e-Signature risk assessment to determine the appropriate signing process. See IRM 10.10.1.3.1.4, Identifying and Authenticating the Signer.
- (5) The e-Signature risk assessment process is used to assess risks associated with the likelihood of a successful challenge to the validity of an electronic signature.

- (6) Per the UESFOT, the risks related to enforceability of an electronic signature analysis must include:
 - a. The likelihood of a successful challenge to the validity of the electronic signature.
 - b. The monetary loss, or other adverse impact, that will result from such a successful challenge to the enforceability of the electronic signature.
- (7) NIST SP 800-53 (Rev. 5), Appendix C, outlines security and privacy controls designed, within an effective risk management framework, to implement fundamental safeguards and countermeasures necessary to protect information during processing, while in storage, and during transmission.

Exhibit 10.10.1-1 (12-03-2019)

Current Approved Methods

The following signature methods have been approved in earlier IRS regulations, publications, or other documents and continue to be accepted by the IRS under current IRS guidance:

Signature Method	Applicable IRS Form
Selecting a checkbox on an electronic device such as a computer or tablet	<ul style="list-style-type: none"> Form 8655, Reporting Agent Authorization
Inputting a PIN	<ul style="list-style-type: none"> Form 720, Quarterly Federal Excise Tax Return Form 940, Employer's Annual Federal Unemployment (FUTA) Tax Return Form 941, Employer's Quarterly Federal Tax Return Form 990, Return of Organization Exempt From Income Tax Form 1040, U.S. Individual Income Tax Return Form 1042, Annual Withholding Tax Return for U.S. Source Income of Foreign Persons Form 1065, U.S. Return of Partnership Income Form 1120, U.S. Corporation Income Tax Return Form 2290, Heavy Highway Vehicle Use Tax Return Form 4506-T, Request for Transcript of Tax Return Form 8849, Claim for Refund of Excise Taxes Form 8878, IRS e-file Signature Authorization for Form 4868 or Form 2350; and those forms in the Form 8878 family Form 8879, IRS e-file Signature Authorization; and those forms in the Form 8879 family
Inputting a Security Code and an Authorization Code	<ul style="list-style-type: none"> Form 720-CS, Carrier Summary Report Form 720-TO, Terminal Operator Report
Using an electronic signature pad	<ul style="list-style-type: none"> Form 8878, IRS e-file Signature Authorization for Form 4868 or Form 2350, and those forms in the Form 8878 family Form 8879, IRS e-file Signature Authorization; and those forms in the Form 8879 family.
Using a stylus device	<ul style="list-style-type: none"> Form 4506-T, Request for Transcript of Tax Return Form 8655, Reporting Agent Authorization ACH Direct Pay
Using voice signature technologies	<ul style="list-style-type: none"> Form 8850, Pre-Screening Notice and Certification Request for the Work Opportunity Credit
Using a scanned or digitized image of a hand-written signature	<ul style="list-style-type: none"> Form 8879-F, IRS e-file Signature Authorization for Form 1041

Exhibit 10.10.1-2 (08-12-2024)**Deviation from Handwritten Signature Requirement for Limited List of Tax Forms Memorandum**

The forms to which this flexibility applies are listed below. These forms must be signed and postmarked on August 28, 2020, or later. Electronic and digital signatures appear in many forms when printed and may be created by many different technologies. No specific technology is required for these forms.

- Form 11-C, Occupational Tax and Registration Return for Wagering.
- Form 637, Application for Registration (For Certain Excise Tax Activities).
- Form 706, U.S. Estate Tax Return.
- Form 706-A, United States Additional Estate Tax Return.
- Form 706-GS (D), Generation-Skipping Transfer Tax Return for Distributions.
- Form 706-GS (D-1), Notification of Distribution from a Generation-Skipping Trust.
- Form 706-GS (T), Generation-Skipping Transfer Tax Return for Terminations.
- Form 706-NA, U.S. Estate (and Generation-Skipping Transfer) Tax Return.
- Form 706-QDT, U.S. Estate Tax Return for Qualified Domestic Trusts.
- Form 706 SCHEDULE R-1, Generation-Skipping Transfer Tax.
- Form 709, United States Gift (and Generation-Skipping Transfer) Tax Return.
- Form 730, Monthly Tax Return for Wagers.
- Form 1066, U.S. Real Estate Mortgage Investment Conduit (REMIC) Income Tax Return.
- Form 1120-C, U.S. Income Tax Return for Cooperative Associations.
- Form 1120-FSC, U.S. Income Tax Return of a Foreign Sales Corporation.
- Form 1120-H, U.S. Income Tax Return for Homeowners Associations.
- Form 1120-IC DISC, Interest Charge Domestic International Sales – Corporation Return.
- Form 1120-L, U.S. Life Insurance Company Income Tax Return.
- Form 1120-ND, Return for Nuclear Decommissioning Funds and Certain Related Persons.
- Form 1120-PC, U.S. Property and Casualty Insurance Company Income Tax Return.
- Form 1120-REIT, U.S. Income Tax Return for Real Estate Investment Trusts.
- Form 1120-RIC, U.S. Income Tax Return for Regulated Investment Companies.
- Form 1120-SF, U.S. Income Tax Return for Settlement Funds (Under Section 468B).
- Form 1127, Application for Extension of Time for Payment of Tax Due to Undue Hardship.
- Form 1128, Application to Adopt, Change or Retain a Tax Year.
- Form 2678, Employer/Payer Appointment of Agent.
- Form 3115, Application for Change in Accounting Method.
- Form 3520, Annual Return to Report Transactions with Foreign Trusts and Receipt of Certain Foreign Gifts.
- Form 3520-A, Annual Return of Foreign Trust with a U.S. Owner.
- Form 3911, Taxpayer Statement Regarding Refund.
- Form 4421, Declaration – Executor's Commissions and Attorney's Fees.
- Form 4768, Application for Extension of Time to File a Return and/or Pay U.S. Estate (and Generation-Skipping Transfer) Taxes.
- Form 8038, Information Return for Tax-Exempt Private Activity Bond Issues.
- Form 8038-G, Information Return for Government Purpose Tax-Exempt Bond Issues.
- Form 8038-GC; Information Return for Small Tax-Exempt Governmental Bond Issues, Leases, and Installment Sales.
- Form 8283, Noncash Charitable Contributions.
- Form 8453 series, Form 8878 series, and Form 8879 series regarding IRS e-file Signature Authorization Forms.
- Form 8802, Application for United States Residency Certification.
- Form 8832, Entity Classification Election.
- Form 8971, Information Regarding Beneficiaries Acquiring Property from a Decedent.
- Form 8973, Certified Professional Employer Organization/Customer Reporting Agreement.
- Elections made pursuant to Internal Revenue Code Section 83(b).

Exhibit 10.10.1-3 (10-17-2023) Glossary and Acronyms

The following table contains key terms, acronyms and definitions used in this IRM.

Term	Definition
A3	Authentication, Authorization, and Access
Authentication	The process of establishing or confirming that someone is the previously identified person they claim to be.
BOD	Business Operating Division
CFR	Code of Federal Regulations
Compliant e-Signature	An electronic signature which meets the five core requirements outlined in IRM 10.10.1.3.1, Requirements for Legally Binding Electronic Signatures: <ul style="list-style-type: none"> • Acceptable forms of electronic signature • Intent to sign the electronic record • Attachment or association of the electronic signature with the electronic record • Identifying and authenticating the signer • Preserving the integrity of the signed electronic record
Digital Signature	A type of electronic signature that uses advanced features and encryption to validate the authenticity and validity of an electronic record.
Digitalization	The process of converting (i.e., scanning) original source materials in analog, or physical format (e.g., paper) to an electronic or digital format of the record. The digitalization process includes planning, assessing, preparing, digitizing, documenting metadata, running quality control checks, validating, storing and managing the digitized records.
Digitized Signature	A digitized image of a handwritten signature.
DIRA	Digital Identity Risk Assessment
EEFax	Enterprise Electronic Fax
Electronic Record	A record created, generated, sent, communicated, or stored by electronic means.
Electronic Signature Pad	An electronic device with a touch sensitive screen that allows users to acquire and register a signature, or any other physical signature capture device that captures and converts a signature into an electronic format.

Exhibit 10.10.1-3 (Cont. 1) (10-17-2023)
Glossary and Acronyms

Term	Definition
Electronic Signing Process	The overall set of actions, steps, and elements used to create a valid and enforceable electronic signature. It includes: <ul style="list-style-type: none"> • The application to an electronic record of a form of signature (i.e., the sound, symbol, or process) to be used as the electronic signature. • One or more processes or security procedures to address the other signature requirements identified in IRM 10.10.1.3.1.4, Identifying and Authenticating the Signer.
Electronic Transaction	The transfer of one or several documents between an external customer and the IRS using computer- mediated networks.
E-SIGN	Electronic Signatures in Global and National Commerce Act
FOD	Functional Operating Division
GPEA	Government Paperwork Elimination Act
GRS	General Records Schedules
IA	Identity Assurance
Identity Proofing	The process of providing sufficient information (e.g., identity history, credentials, documents) to establish an identity.
IRC	Internal Revenue Code
IRM	Internal Revenue Manual
IRS Document	Any return, statement, or other document made under any provision of the Internal Revenue Code, published guidance, publications, forms, instructions, online applications, or on the IRS website.
IT	Information Technology
JPEG	Joint Photographic Experts Group
NARA	National Archives and Records Administration
NCCUSL	National Conference of Commissioners on Uniform State Laws
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
Password	A secret word or string of characters that is used for authentication, to prove identity, or gain access to a resource.
PDF	Portable Document Format
PGLD	Privacy, Governmental Liaison and Disclosure
PIN	Personal Identification Number
RAFT	Risk Assessment Form and Tool
RCS	Records Control Schedule

Exhibit 10.10.1-3 (Cont. 2) (10-17-2023)
Glossary and Acronyms

Term	Definition
SP	Special Publication
Stylus Device	A device used on a display screen to input commands or handwritten text.
TIFF	Tagged Image File Format
UESFOT	Use of Electronic Signatures in Federal Organization Transactions
UETA	Uniform Electronic Transactions Act

