Adobe Sign

Get set for e-signature success.

Developing an effective electronic signature policy.

Electronic signatures are transforming the way organizations do business. Not only do they eliminate the hassle of manually routing paper agreements, they also speed up signature and approval processes dramatically. Best of all, making electronic signatures a part of your existing workflows is easier than you think. A good place to start is by establishing a master signature policy.

A strong electronic signature policy sets forth the guidelines for using e-signatures and helps ensure your signature processes comply with local and global laws, as well as regulatory guidelines. The first step in creating an electronic signature policy is to determine what elements to include.

This guide outlines some suggestions to help you create an electronic signature policy that works across your organization. The following are some considerations for developing a policy that ensures your electronic agreements are legal and enforceable.

Understand e-signature laws.

Electronic signatures are legally valid and enforceable in nearly every industrialized country around the world. But since electronic signature laws vary from country to country, it's a good idea to develop a corporate electronic signature policy that will work in all the countries where you do business. Before you begin to create your policy, it's important to understand the various electronic signatures laws and how they may impact your use of e-signatures locally and internationally.

Worldwide, there are generally two types of electronic signature laws:

- **Minimalist laws**—Many countries, including the United States, Australia, New Zealand, and Canada, have minimalist or permissive laws, which allow for the broad enforceability of e-signatures with few legal restrictions and give e-signatures the same legal status as handwritten signatures.
- **Multitier laws**—Countries with multitier laws generally permit the broad use of e-signatures, but provide greater evidentiary weight to signatures that use different types of certificate-based digital IDs to authenticate signers. Regions and countries that have adopted multitier laws include the European Union, China, India, and South Korea. In the European Union, for example, only signatures using digital IDs from qualified providers are automatically given the same status as handwritten signatures.

Professional electronic signature solutions like Adobe Sign make it easy to comply with both minimalist and multitier laws and support business processes across multiple countries.

Find a signature approach that fits.

An important step in drafting an electronic signature policy is to evaluate your agreements to find the right signature approach for your business. You'll need to balance regulations and risk and consider what level of effort is necessary to make your business transactions both legal and secure. There are different factors to consider depending on your specific business processes and the local laws and regulations that govern them. Still, well-constructed electronic signature processes typically use one or more of the following methods to automate signature processes and ensure compliance.

- **Low risk: Standard e-signatures**—Where business risk isn't high and the law allows it, many organizations use standard e-signatures for everyday business agreements such as contracts, statements of work, or employee forms. Using a secure signing process, an email request is sent to each signer. The signer simply clicks the unique link embedded in the email to access the document. Because most people have unique access to one email account, this serves as a basic method of signer authentication. The document is managed securely throughout the process and each step in the process—including authentication—is logged and stored in an audit trail.

After everyone has signed, the final document is sent to all parties automatically, complete with a tamper-evident seal to confirm its integrity. To further enhance legal compliance, organizations can also build processes that require explicit consent to do business electronically before engaging in the signature process.

- **Moderate risk: Enhanced e-signatures**—To strengthen security, many organizations add a second form of signer authentication on more sensitive agreements. Enhanced e-signatures work just like standard e-signatures, but add a signer authentication challenge before a document can be opened or signed. Using methods such as phone PINs, social IDs, passwords, or knowledge-based authentication (KBA), the identity of signers can be verified with very high levels of assurance.
- **High risk or mandated by regulation: Digital signatures**—To meet the most stringent legal and regulatory compliance requirements—and protect the highest risk, highest value signing processes—some organizations choose digital signatures.

  Digital signatures are a very specific type of electronic signature that use certificate-based digital IDs to authenticate signer identity. These IDs are typically issued by a Certificate Authority (CA) or Trust Service Provider (TSP). Like their e-signature counterparts, digital signature solutions can include audit trails, automatic delivery of the final document, and options for explicit consent. Proof of signing is different, however, because the signature itself is bound to the document with encryption, and can be validated through the CA or TSP long after the document has been signed.

To determine which approach works best for your company's e-signature needs, you may want to ask yourself some key questions about your business processes:

- Does any applicable law demand a specific form of signature?
- Am I willing to invest in equipping all signers with digital IDs?
- What's the likelihood this signature may be challenged and what's the risk associated with that?
- Would the requirement for a digital ID become a roadblock for average customers?

Build best practices into your policy.

All e-signature laws share common fundamental principles, so whether you're doing business in just one country or many, there are six key questions your signature policy will want to address to ensure that your electronic agreements are legal and enforceable.

1. **Authentication:** Who signed?
2. **Intent to sign:** Did the signer demonstrate intent to sign?
3. **Proof of signing:** Can you prove a specific document was signed and hasn't been altered since signing?
4. **Consent:** Did the signer consent to do business electronically?
5. **Exceptions:** Are there any excluded document types?
6. **Retention:** How long should your records be stored?

Authenticate signer identity.

Your electronic signature process should ensure signers can be identified and authenticated during the signing process. Most organizations choose one or more of the methods described in the previous section, depending upon the risk and compliance requirements for their business processes. Adobe Sign supports all of these methods in one solution, making it easy to choose the right approach for each process.

Demonstrate intent to sign.

Your processes should include a step where the signer takes a clear action during the process (e.g., typing or drawing a name or clicking a button) to establish intent to be bound. Signers should also be given the chance to opt out of signing an agreement electronically. Both of these functions are built into Adobe Sign processes.

Establish proof of signing.

In order to qualify as an electronic signature, a signature must be associated with the document that was signed.

That's why Adobe Sign manages documents securely throughout the signing process and certifies signed documents with a tamper-evident seal to confirm their integrity. Each step is captured in a secure audit trail that provides clear, easily producible evidence of each party's signature. Once a document has been signed, all signers receive an unaltered, fully executed electronic copy of the agreement for their reference and archiving.

Consent to do business electronically.

Many electronic signature laws require some form of consent to do business electronically. Electronic signature solutions like Adobe Sign have consent built into the workflow, so you don't need to alter your documents. However, you still may want to include additional language in the body of the agreement itself, so consider adding a consent clause to your agreements. For example, your agreements could include the following clause right above your signature block:

> **Please read the following information:** By signing this document, you are agreeing you have reviewed this consumer disclosure information and consent to transact business using electronic communications, to receive notices and disclosures electronically, and to utilize electronic signatures in lieu of using paper documents. You are not required to receive notices and disclosures or sign documents electronically. If you prefer not to do so, you may request to receive paper copies and withdraw your consent at any time.

Call out exceptions.

Some processes can't be executed electronically. If you have particular agreements you want to exclude or include, regardless of your general policy, add a section that details those exceptions. Some electronic signature laws, for instance, exclude real-property transfers and family law agreements. And some highly regulated industries, such as biopharma, will only accept digital signatures for certain business process types. Your risk analysis helps you determine which exceptions to include in your policy.

Hold on to records.

Treat your electronic signature documents just like you would any other documents. That includes determining how long your records need to be retained. Electronic signature transaction records typically need to be kept for the same length of time as documents signed in ink. Be sure to review and adhere to any laws that apply to your organization's record retention policy. Records must remain accessible in a form that can be reproduced by anyone entitled to access the record (e.g., the signer). Adobe Sign stores records securely in Adobe Document Cloud. If you have important high-risk documents, you may also want to consider archiving them in a formal records management system or an e-vault system.

Draft a clear policy.

Once you know what your policy should say, it's important to make it easily understandable for your users. Here are three tips to help you write a policy that people will actually read.

State the objective of your policy.

Define the purpose or objective of your policy. An example might be, "This policy provides guidelines for the adoption of electronic signatures, including defining the circumstances under which electronic signatures and records will be used and accepted."

Summarize your policy.

Include a summary of your policy. This could be a short statement acknowledging your organization's decision to accept electronic signatures, approvals, or authorizations required for the purpose of conducting business as legally binding and equivalent to a handwritten signature. If there are certain conditions under which electronic signatures are acceptable and when they are not (e.g., agreements you want to exclude or include, departments not authorized to use electronic signatures, and so on), you will want to call out those exceptions in your policy statement.

Define the terms used in your policy.

Define commonly used terms so everyone is clear on what you mean by the language used in your policy guidelines. You'll find some common definitions in the Appendix.

Communicate your policy.

Once everything is finalized, it's important to communicate your policy throughout your organization so everyone knows how and when to use e-signatures in their workflows. Publish your policy in a place that is easy to access. Consider rolling it out at a live meeting or event, so you can explain it and answer questions. Finally, check your organization's implementation—including any standard document or workflow templates—to ensure they are consistent with your new policy.

Find out more.

To learn more about e-signatures, consult these resources:

- Global Guide to Electronic Signature Law: Country by Country
- Transform business processes with electronic and digital signatures
- Electronic Signatures in Law

Appendix: Electronic signature terminology.

Electronic signatures or **e-signatures** mean any electronic process that indicates acceptance of an agreement or a record. Electronic signatures may use a wide variety of methods to authenticate signer identity.

Standard e-signature systems combine a single electronic authentication method—such as access to an email account—with a secure process that delivers an audit trail along with the final document.

Enhanced e-signatures add multifactor authentication to verify the identity of the signer. First, signers access a URL uniquely sent to their email account, and then they complete a challenge before opening the document. Commonly used challenges include phone PINs, social IDs, passwords, or knowledge-based authentication (KBA).

Digital signatures are a specific type of electronic signature that use a certificate-based digital ID to authenticate signer identity. Digital signatures demonstrate proof of signing by binding each signature to the document with encryption. Validation is typically done through trusted Certificate Authorities (CAs) or Trust Service Providers (TSPs).

Certificate Authorities (CAs) are trusted companies or IT-provided services that issue and maintain digital identities. CAs confirm a signer's identity in advance, and then issue the digital ID, private PIN, and/or hardware security device (such as a USB token or smart card) used to create digital signatures.

Trust Service Providers (TSPs) are companies that offer a wide range of secure identity and transaction services, including CA services. For example, the EU eIDAS regulation defines a class of TSPs that are accredited to issue digital IDs in each of the EU member states. Documents signed with these IDs meet the highest level standard called "Qualified Electronic Signatures," which has the same legal value as handwritten signatures.