

# Developing an effective electronic signature policy



Electronic signatures, or e-signatures, are transforming the way companies do business. Not only do they eliminate the hassle of manually routing paper agreements, but they also dramatically speed up the signature and approval process. Implementing e-signatures into your existing workflows is easier than you think. A good place to start is by establishing a master signature policy.

A successful e-signature policy includes clear guidelines, such as:

- · Types of agreements to authorize for e-signatures
- · Best practices to implement
- · Disclosures to include in different types of agreements
- · Global regions in which to use e-signatures

This white paper walks you through those guidelines to help you create an e-signature policy that works across your company.

# Evaluate your agreements

The first step in drafting an e-signature policy is to determine which types of agreements work best for e-signatures. While e-signatures work well for most agreements, you need to consider factors like the monetary value of sales and procurement agreements, the governing laws of all involved parties, and other risk factors.

Some companies are more risk-adverse than others. So conduct a risk analysis to decide the types of agreements that make sense for your company's e-signature workflow. If your company wants to pilot e-signatures, you can start by implementing low-risk agreements, such as nondisclosure agreements or domestic sales and procurement agreements under a certain currency value. If, on the other hand, you want to roll out e-signatures more broadly, your policy can cover a diverse range of agreements and exclude only certain types of agreements, like real estate transfers, legally required consumer notices, or agreements that require notarization. You can also specify that even more critical agreements, such as high-value sales contracts, require more robust signer authentication, so you can include as many agreements as possible in your e-signature workflow while mitigating risk. If you are considering using e-signatures for some agreements and digital signatures—signatures that attach a digital certificate for authentication—for other agreements, consider creating a table to identify which signature is acceptable for each type of agreement.

# Choose best practices and required disclosures

Your policy should also include specific best practices and disclosures. Some disclosures are required by law. Evaluate your company's agreements and your local laws to determine which disclosures are required for your business, and adopt best practices that support those requirements. The following are some suggestions to consider:

## Consent to do business electronically

Most e-signature laws require some form of consent to do business electronically. Many enterprise e-signature solutions have some form of this consent built into the e-signature workflow, so you don't need to alter your documents. However, you may want to include additional language, 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 that you have reviewed the following 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.

## **Opt-out clause**

Signers should be given an opportunity to opt out of signing an agreement electronically. Your policy should address the procedures that signers who elect to sign an agreement by hand should follow.

### Governing law and venue

Worldwide, there are generally three types of e-signature laws:

- "Minimalist" laws allow for the broad enforceability of e-signatures with few legal restrictions.
- "Two-Tier" laws generally permit the use of e-signatures but provide greater evidentiary weight to digital signatures.
- "Prescriptive" laws dictate specific technical methods to electronically sign a document.

Many countries, including the United States, Australia, New Zealand, and Canada, have minimalist laws, which provide the widest protection for e-signatures. Because of this, it is advisable to choose the governing laws of one of these countries in your agreements to provide an additional assurance that the e-signature is enforceable in the case of a dispute.

#### Advanced authentication

Some companies find it helpful to use advanced authentication options, like knowledge-based authentication, customized passwords, or phone authentication, for higher risk agreements. Knowledge-based authentication requires signers to prove their identity by answering questions unique to them. The questions are based on data available in public and commercial databases. You can also authenticate signers by creating a secure, unique password they must enter before they sign. Phone authentication is also effective. To sign, users must enter a one-time verification code that is delivered to their phone via voice or text message.

#### Signed copies

All signers should receive a fully executed copy of the agreement. Many enterprise e-signature solutions automatically provide executed copies of agreements to signers as part of the signature workflow. These workflows are easily customizable, so you can choose the process that works best for your organization.

## Call out exceptions

If you have particular agreements you want to exclude or include, regardless of your general policy, add a section that details those exceptions. For example, you may want to exclude agreements involving highly regulated industries, real-property transfers, or family law. Your risk analysis helps you determine which exceptions to include in your policy.

## Communicate your policy

When you have completed your e-signature policy, make sure you check your agreement templates to ensure they are consistent with your new policy. Once everything is finalized, it's important to communicate your policy throughout your company so everyone knows how and when to use e-signatures in their workflows. Publish your policy in a place that is easy to access, and consider rolling it out at a live meeting or event so you can explain it and answer questions. The key to adoption is effective communication.

#### For more information

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

- Global Overview of Electronic Signature Law
- Global Guide to Electronic Signature Law: Country-by-Country
- Transform business processes with electronic and digital signatures
- Adobe Sign Solution Brief



Adobe is pleased to provide information that can help businesses understand the legal framework of electronic signatures. However, Adobe cannot provide legal advice. Any information in this paper is not intended as legal advice and should not serve as a substitute for professional advice. You should consult an attorney regarding your specific legal questions.

4/16

Adobe Systems Incorporated 345 Park Avenue