Electronic Signature Policy

This policy establishes when an electronic signature may replace a written signature and when an electronic record may replace a paper document.

This policy applies uniformly and governs all uses of electronic signatures and electronic records. Such business shall include, but not be limited to, electronic communications, transactions, contracts, grant applications, and other official purposes.

POLICY

The policy allows the use of electronic signatures as an acceptable alternative to an original signature for those documents requiring signature or acknowledgement in accordance with minimum standards. This policy is intentionally flexible.

Note: The policy does not mandate the:

- use of an electronic signature
- method or software utilized for any specific need, so long as the method adopted conforms to the minimum standards outlined in this policy
  (See Technology Guidelines below)

MINIMUM STANDARDS

Use of an electronic signature must be in accordance with the following minimum standards, consistent with NH State issued guidelines. Compliance with these standards helps to ensure the validity of an electronic signature.

Step	Action
Preparation	1. Obtain approval from CDFA to implement the use of electronic signatures. 2. Determine that electronic signature methodology will be made in accordance with the specific standards outlined in this policy.
Processing	1. Provide opportunity for the signer to review the entire document or content to be signed prior to applying an e-signature. 2. 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.

Step	Action
	3. 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.
Signature Retention	1. 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. 2. Retain all electronically signed documents in accordance with CDFA's Record Retention Policy.

SECURITY AND RISK

Organizations that choose to use electronic signatures must ensure a proper level of security and ability to link the signed document with the signer. This policy does not supersede any law or scenario wherein a written signature is specifically required.

PLEASE NOTE: AS OF JUNE 2019, ALL CONTRACTUAL DOCUMENTS WITH THE STATE OF NEW HAMPSHIRE REQUIRE AN ORIGINAL WRITTEN SIGNATURE.

Various technologies support different levels of security, authentication, record integrity and record retention. Solutions for making an electronic signature trustworthy must address the following security concerns:

Function	Provides
Confidentiality	Protects content from unauthorized access so that only the intended audience can view it
Authenticity	Assures that the document truly comes from the signer
Integrity	Detects unintentional or malicious alteration and prevents signer from refuting an electronic signature document
Security	Maintains security of document from origination through the entire business process
Accessibility	Allows access to document across all platforms

CDFA recommends that organizations that are considering using electronic signatures:

- perform and document an internal risk assessment to assist with identifying the risk(s) around the objective(s) including but not limited to compliance, potential legal issues, and significance
- evaluate business and technological solutions against their potential to mitigate risk

TECHNOLOGY GUIDELINES

There are a number of approaches to implementing the use of electronic signatures. The technology approach selected should support the minimum standards outlined in this policy. When choosing a technology, consider the significance of the business requirement as it relates to electronic signatures. For instance, applying an electronic signature to an e-mail might be fine, but additional validation or security in other situations may necessitate password protection or encryption. A combination of technologies may be warranted to mitigate risks.

Examples of technology that support digital signatures that may work for various CDFA related projects or documents include:

Technology Approach	**Provides that signer or signature is …**
Click Through or Click Wrap	asked to click a button to demonstrate intent
Personal Identification Number (PIN) or Password	asked to enter identifying information
Signature Dynamics	authenticated through automated analysis
Biometrics	authenticated by physical characteristics prior to applying his or her signature
Shared Private Key (Symmetric) Cryptography	authenticated by using a single cryptographic key (encrypts and decrypts message). This method should only be used if the keys are changed regularly to ensure a higher level of security
Public/Private or Asymmetric Cryptography (PKI) – Digital Signature	authenticated by using two cryptographic keys one private and one public (encrypts and decrypts message)

Note: Other methods may be developed which incorporate applicable minimal standards, this list is not meant to be inclusive. Please contact CDFA if any other methods are proposed.

CERTIFICATION PRACTICE STATEMENT

A Certification Practice Statement (CPS) is a statement or policy describing the compliance practices of a certificate authority concerning his or her digital certificates.

A standard CPS outlines	**An excellent CPS includes**

Digital certificate authority concerning	Digital certificate authority concerning
• issuing • renewing • revoking • validation	• all standard CPS content • liabilities • financial responsibilities • governing laws • compliance/audit standards and frequencies

Whenever feasible, a CPS should be obtained from either the:

- vendor providing digital certificate services to the organization, or
- responsible administration that manages the service when an organization provides their own certificate services infrastructure