Potsdam
STATE UNIVERSITY OF NEW YORK

Electronic Signature Policy

Definitions

The following terms are used in this policy.

Term	Definition
Electronic Signature	An electronic signature is a paperless method used to authorize or approve documents which indicates that a person adopts or agrees to the meaning or content of the document. Federal (the federal E-Sign law) and New York state law (The Electronic Signatures and Records Act or "ESRA") define 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."

Basis for Policy

The following laws were enacted to support the use of electronic signatures.

Law	Definition
Federal Law	The federal government authorized the use and acceptance of electronic signatures in The Electronic Signatures in Global and National Commerce Act (E-Sign).
NYS Law	The Electronic Signatures and Records Act (ESRA), the New York state law which authorizes the acceptance of electronic signatures in most documents, went into effect in August of 1999. The Act was updated in 2002 to make New York state law consistent with the federal E-Sign law. The act provides that "signatures" made via electronic means will be as legally binding as hand-written signatures. It does not mandate the use of, or require a specific form of, electronic signature.

Those choosing an electronic signature method can be assured that the electronic signature will be given full legal effect under federal and state law if the signature method conforms to the standards outlined in the policy.

Exceptions

E-Sign and ESRA contain exceptions to the general standard that electronic signatures are afforded full legal effect. These exceptions indicate when an electronically signed document is not afforded the same legal standing as a handwritten signature. Most of these exceptions would not apply to the College. In general, a handwritten signature may be required for documents or notices pertaining to:

- the transfer of real property
- eviction and foreclosure
- cancellation of health insurance
- the Uniform Commercial Code.

Policy

The College 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.

Note: The policy does not mandate the

- use of an electronic signature
- application to those internal operational type documents which require an informal routing or acknowledgement
- 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)

This policy does not allow for acceptance of signatures in electronic form for the release of student records pursuant to the federal Family Education Rights and Privacy Act (20 U.S.C. §1232g).

Prior to electing to use or accept an e-signature solution, the College must conduct and document a business analysis and risk assessment. Business analysis and risk assessment is defined by the ESRA 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.”

Minimum Standards

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

Step	Action
Preparation	1. Obtain approval from President's Council 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. 3. Verify that electronically signed documents going to external agencies abide by guidelines set forth by the external agency and meet the requirements of the receiving organization.
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. 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 the State University of New York's Records Retention and Disposition Policy.

Implementation

Security and Risk

The College 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 (see above for specific exceptions).

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 prevent signer from refuting a electronic signature document
Security	Maintains security of document from origination through the entire business process
Accessibility	Allows access to document across all platforms

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 College 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.

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 • issuing • renewing • revoking • validation	Digital certificate authority concerning • 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 College
- responsible administration that manages the service when a department provides their own certificate services infrastructure

For more detailed best practice and technology guidelines, refer to the New York State Office for Technology Web site NYS Best Practice Guideline and NYS OFT Policy PKI Certificate.

The National Institute of Standards and Technology (NIST) Electronic Authentication Guidelines: 800-63 guidelines may also be used to help determine methodology.

Responsibilities

This policy identifies the following responsibilities as assigned to those cited below.

Role	Individual/Group	Contact Information
Comply with	All College staff	n/a
Policy Executor(s)	Romeyn Prescott, Acting Chief Information Officer (CIO) Computing & Technology Services	(315) 267-3181 cio@potsdam.edu

Change History

Date	Change History
1/9/2018	New Policy.

Effective Date: 1/9/2018

Responsible Party: Romeyn Prescott

Contact Information: (315) 267-3181