RUTGERS
THE STATE UNIVERSITY
OF NEW JERSEY

RUTGERS SCHOOL OF ARTS AND SCIENCES
DIGITAL SIGNATURE POLICY

Section:

Section Title: Information Technology

Policy Name: Digital Signatures

Approval Authority: SAS Executive Dean

Responsible Executive: Executive Director of Information Technology

Responsible Office: SAS IT Office

Originally Issued:

Revisions:

1. **Policy Statement**

   This policy governs the use of digital signatures and specifies when they may be used, the functional requirements of the digital signature system, and the method of user interaction with the system. It also specifies conditions for users to opt out and continue to use physical signatures.

2. **Reason for Policy**

   To ensure that digital signatures are implemented in a consistent way across the School of Arts and Sciences and in a fashion that is in compliance with all University policies and established legal requirements.

3. **Who Should Read This Policy**

   This policy applies to any individual who is involved with any process that has been approved to use digital signatures.

4. **Related Documents**

   NJ Uniform Electronic Transactions Act -
   http://www.njleg.state.nj.us/2000/Bills/PL01/116_.PDF

5. **Contacts**

   info@sas.rutgers.edu

6. **The Policy**

   A. Implementation of Electronic Signatures

      In order for digital signature systems to be reliable, they must be implemented in a consistent way. Consistency is required in both the interface that is presented to the user and in the algorithm that is used to both sign and store the digitally signed documents.

a. Ability to Opt Out

Systems that are permitted to use digital signatures must provide users with the ability to opt out of the digital signature system and sign the documents in traditional fashion. Users should be given the ability to print the form, sign it manually, and then submit it.

b. Notification that Electronic Signatures are Legally Binding

Before signing any document electronically, users will be presented with language provided by University Counsel that informs them that the digital signature is as legally binding as a manual signature. Users will be required to affirm that they have read and understood.

c. Separate Authentication or Action Requirement

When digitally signing a document, users must take additional positive action in the software to have their signature entered. For example, users must re-enter their authentication password or type in a short word or phrase like “AGREED”. Simply clicking on a single button is not sufficient to serve as affirmation of a digital signature.

d. Copy Must Be Available to Signee

Once the document has been digitally signed, the user must be given the option to either download or have e-mailed, a copy of the digitally signed document. The signature will be represented by a unique key that, if permitted by policy, can also be used to retrieve the document from the digital signature archive.

e. Ability to Verify Signature

i. The digital signature system will have a mechanism to verify the signature on a document. The signee will be able to use the copy of the document that was downloaded to re-generate the signature key. If the document has not been changed, the signature key that is generated by the software will be identical to the one that was sent to the user and stored by the system.
ii. The digital signature will be generated using a specific algorithm that must be kept private to prevent signature forgeries. The method that is used will not be disclosed unless required by law.

f. Modification of Document must Invalidate Signature

The digital signature system will store a generated key that will uniquely identify the document. This key will be used in conjunction with each signee’s identity, in the form of their RCPID, to create a secondary key that will uniquely identify the document as signed by each person. If the document were to change in any way, both the document key and the signature keys would become invalid.

B. Obtaining Authorization for Digital Signatures

a. SAS Dean’s Office

To request that an additional document be authorized for digital signatures, the document must be submitted to the SAS Dean's Office for approval. The document will be reviewed by the SAS IT Office and by the Office of Administration who will recommend a course of action to the Executive Dean.

b. Form Owner Approval

If the form originates outside of the SAS, approval for the use of digital signatures will be sought from the originating area.

c. University Counsel

University Counsel will review submitted documents and then either approve or deny the use of digital signatures. If approved, counsel's office will also specify whether or not users are permitted to look up the signed document using the signature key that is provided to the signee.

C. Limitation on Deployment of Digital Signature Systems

The digital signature system maintained by the SAS Information Technology Office will be the only digital signature system deployed in the School of Arts and Sciences.