19.4.1 Electronic Signatures

Policy Statement

The University of Illinois may provide and accept an electronic signature as legally binding and equivalent to handwritten signatures to a contract as permitted by law. An electronic signature is defined as a signature in electronic form attached to or logically associated with an electronic record.

Units seeking to provide and accept electronic signatures must:

1. Comply with conditions for providing identity assurance, such as, authenticating the identity of the user through university systems or additional levels of authentication as required.
2. Ensure that the signature and all necessary verification records are maintained for the full life cycle of the contract and contract records.

An electronic signature that does not meet these criteria at the time of signature may not be binding on the University of Illinois.

Reason for the Policy

The Electronic Commerce Security Act (5 ILCS 175/25-101) provides that a state agency may decide the extent to which it will send and receive electronic records and electronic signatures to and from other persons and otherwise create, use, store, and rely upon electronic records and electronic signatures.

Applicability of the Policy

This policy applies to all University of Illinois contracts.

Procedure

Units seeking to provide and accept electronic signatures should assess the risks associated with related transactions. Part of this process involves selecting a signature authorization method that provides appropriate levels of identity assurance. Units should consult the system's Identity Assurance Guide and discuss electronic signature acceptance options, such as AdobeSign, with appropriate information technology units.

Units must also ensure that the signature and all necessary verification records are maintained for the full retention period under the RIMS Records Retention Schedules. The verification records, such as the Audit Report available within AdobeSign, for documents containing electronic signatures that were internally routed (exclusively within the System) should be maintained by the unit that accepts the final document. The verification records for documents containing electronic signatures that were externally routed (includes one or more non-system parties) should be maintained by each internal (System) unit that electronically signed the document. Individuals who

sign contracts on behalf of the Comptroller must have express authority to do so consistent with 19.4 Comptroller Contract Signature Authority and Delegation. A signature is defined in the same manner as in the State of Illinois Electronic Commerce Security Act (5 ILCS 175/5-105) as any symbol executed or adopted, or any security procedure employed or adopted, using electronic means or otherwise, by or on behalf of a person with intent to authenticate a record.

Comptroller delegates who sign contracts using an electronic signature method are responsible for compliance with this policy. Delegates must ensure that the signature block of a contract contains all required information, as documented in 19.4 Comptroller Contract Signature Authority and Delegation. In addition, if digital signatures are used, the digital signatures must comply with digital signature requirements of Illinois law.

Units that are responsible for processing contracts may accept electronic signatures from the other party so long as the unit determines that the signature is affixed in a trustworthy manner and presents a reasonable level of reliability and authenticity (Identity Assurance Guide).