Northeastern University

Policy on Use of Electronic Signatures

BUSINESS AND FINANCIAL AFFAIRS

Effective Date:
September 19, 2013

Date Revised: N/A

Supersedes: N/A

Related Policies:
Policy on Appropriate Use of Computer and Network Resources
Policy on Signature Authority
Records Management Policy and Procedures; Contract Review Policy; Policy on International Agreements

Responsible Office/Department:
Office of Information Security

Keywords: Electronic Signature; Electronic Transaction; E-sign; click-through agreements; authenticated portal

I. Purpose and Scope

Federal and state laws authorize the acceptance of electronic signatures as legal and enforceable for most transactions. Northeastern University recognizes this general standard as well as the increased operational efficiency gained from conducting many business transactions by computer, over the internet, and by e-mail. This policy establishes guidelines for units within the University to authorize the use of electronic signatures to the fullest extent permitted by law, using methods that are secure and practical, after identifying and evaluating the risk for each specific application.

This policy applies to all members of the University community, including students and prospective students, employees and prospective employees, faculty, staff, volunteers in connection with University activities, business partners, affiliates, and associates. It applies to all uses or potential uses of electronic signatures to conduct the official business of the University, including transactions with third-party vendors and contractors.

This policy does not mandate the use of an electronic signature or otherwise limit the right of a party to conduct a transaction on paper, nor does it apply to any situation where a written signature is required by law. The policy does not apply to facsimile signatures used on checks issued by the University.

The policy does not require a specific method for acceptance of an electronic signature, but authorizes each unit, department, or administrative office to implement the method that provides an appropriate level of authentication assurance to address the identified degree of risk in each transaction.

II. Definitions

For purposes of this policy:

Authentication means to establish as genuine and verify the identity of a person providing an electronic signature.

Electronic signature, or "e-signature," is 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. Examples can include a digitized image of a handwritten signature, a code or personal identification number (PIN), and a mouse click on an "I accept" or "I approve" button. An electronic signature must be attributable (or traceable) to a person who has the intent and authority to sign the record with the use of adequate security and authentication measures that are contained in the method of capturing the electronic transaction (e.g., use of PIN or unique log-in username and password), and the recipient of the transaction must be able to permanently retain an electronic record of the transaction at the time of receipt.

Electronic record is any record created, used, or stored in a medium other than paper, including information processing systems, computer equipment and programs, electronic data interchanger, electronic mail, voice mail, text messages, and similar technologies. To the extent that facsimile, telex, and/or telecopying, and/or former hard copy documents are retained in electronic form, through a scanning process, they are also considered electronic records.

Electronic transaction, or "e-transaction," is a transaction conducted or performed, in whole or in part, by electronic means or electronic records. The information provided, sent, or delivered, in an electronic record must be capable of retention by the recipient at the time of receipt to qualify as an electronic transaction.

Approved electronic signature method is one that has been approved by Information Security, in accordance with this policy and applicable state and federal laws, and which specifies the form of the electronic signature, the systems and procedures used with the electronic signature, and the significance of the use of the electronic signature.

Level of Assurance is the degree of confidence in the identity of the individual providing an e-signature.

Approval Authority means a Senior Vice President or designee.

III. Policy

When a signature, approval or authorization is required for a University transaction, by law or by University policy or practice, an electronic signature, approval or authorization will meet the requirement, and will be accepted as legally binding and equivalent to a handwritten signature when:

A. the particular unit, office or department has designated the transaction as an appropriate e-transaction, after analysis of the benefits and risk;

B. the Approval Authority for the particular Unit, office, or department has authorized the use of electronic signature for that transaction; and

C. the unit has implemented an approved electronic signature method and user authentication protocol appropriate to establish the level of assurance needed for the degree of risk identified in the analysis.

Units are encouraged to consult with and use the E-authentication Guidance developed by the United Sates Office of Budget and Management and available at http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdfin determining the level of assurance appropriate to proposed e-transactions, and thus the approved e-signature method required. Units should also consult the E-Signature Guidelines available from the Information Security Office.

IV. Additional Information

As set forth in the University's Appropriate Use Policy, all accountholders are responsible for activities conducted under their user ID, and are expected to take all precautions to safeguard their password and files to prevent unauthorized use. Sharing of passwords or other access tokens is prohibited.

Individuals who falsify e-records, e-transactions or e-signatures are subject to disciplinary action, up to and including termination of employment and criminal prosecution under applicable federal and state laws. Individuals are required to report any suspect or fraudulent activities related to e-transactions, e-records or e-signatures immediately to the Information Security Office and to any manager or supervisor in the individual's department, college or division.

Nothing in this policy is intended to authorize any individual to sign on behalf of Northeastern University if he or she has not been granted such authority, and such signature authority continues to be governed by University bylaws and applicable University policies. The presence of an electronic signature does not mean that the signatory was authorized to sign or approve on behalf of the University.

V. Contact Information

Office of Information Security, OIS@northeastern.edu