WCU
WEST CHESTER UNIVERSITY

UNIVERSITY POLICY

UNDER REVIEW

Acceptable Uses of Electronic Signatures Policy

Accommodations for individuals with disabilities in accessing these policies are available upon request by emailing accessiblepolicy@wcupa.edu

Purpose and Scope

With increased emphasis on paper reduction, there has been increasing interest in fully electronic processing and approvals of documents and workflows. The purpose of this policy is to establish the circumstances in which electronic signatures are considered an acceptable means of signing electronic documents and correspondence at WCU, and thus a substitute for traditional "wet" signatures. This policy also defines some of the basic requirements for an electronic signature in order to allow the recipient a suitable level of trust regarding the signer's authenticity. This policy does not in any way address confidentiality of the documents being signed.

This policy applies only to intra-organization electronically signed documents and correspondence and not to electronic materials sent to or received from non-West Chester University affiliated persons or organizations. This applies to the gathering of electronic signatures in SharePoint in a workflow capacity (approval acknowledgement) only and for situations in which the data collected is deemed not Confidential, based on the Data Classification Policy definition.

Policy Statement

An electronic signature is an acceptable substitute for a wet signature on any intra-organization document or correspondence, with the exception of those noted:

Electronic signatures must apply to individuals only. Electronic signatures for roles, positions, or titles (e.g. the CFO) are not considered valid.

In order for electronic signatures to be in compliance with this policy, the following criteria must be met:

- Password-based signatures should be used in conjunction with at least one of the following: PKI, signature stamps, electronic seals, or simple click-wrap
- Electronic signatures must be verifiable. Electronic signatures should be logged in the system being used for the document. The elements of the log should include at a minimum:
    - User Name
    - Full Name
    - WCU ID Number
    - Date Signed
    - Web Application Name
    - Active Directory SID (optional)
    - Relevant URL of document (optional)
- The signature must be unique to the individual whether it is a physical measurement such as a fingerprint or a virtual measurement such as a mouse click
- The signature must establish the individual's intent to be bound to the transaction. Signatory must be fully aware of the purpose for which the signature is being provided, regardless of underlying technology

Policy Framework

Electronic signature acceptance requires specific action on the part of the employee making a request that requires a signature (hereafter the requester), the employee signing the document or correspondence (hereafter the signer), and the employee receiving/reading the document or correspondence (hereafter the recipient).

Requester Responsibilities

Because signatures are based on authenticating a user, requesters must protect their login credentials and keep them secret.

If a requester believes that his or her login credentials were stolen or otherwise compromised, the requester must contact the IS&T Helpdesk immediately to have the credentials reset.

Requester provides appropriate and accurate name(s) and email address(es) of the person(s) that need to provide the electronic signature(s)

Signer Responsibilities

Because signatures are based on authenticating a user, signers must protect their login credentials and keep them secret.

If a signer believes that his or her login credentials were stolen or otherwise compromised, the signer must contact the IS&T Helpdesk immediately to have the credentials reset.

Signer acknowledges the approval of the request by clicking an approve button or similar method after providing login credentials.

Recipient Responsibilities

Recipients must verify that the signer's identity (username captured during the approval process) matches the name and email address that were provided by the requester.

If the signer's electronic signature does not appear valid, the recipient must not trust the source of the document or correspondence and should take extra steps to either validate the signature with the signer using non-electronic means or deny the request.

If a recipient verifies with the signer that the signature has been abused, the signer must take the appropriate actions specified above regarding stolen credentials.

Policy Exceptions

Any exception to the policy, such as the use of other electronic signature technologies not described here, or the use of electronic signatures in ways that are outside the scope described above, must be approved by IS&T in advance of deployment.

Procedures

The items below are examples of acceptable uses of WCU Electronic Signatures:

Electronic Signature Examples
• Acknowledgement that you read and agree with information presented • Internal IT Requests for Equipment • Approval during a workflow transaction

Definitions

Electronic Signature – "An electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record." [ESIGN Act]. Although all electronic signatures are represented digitally (i.e., as a series of ones and zeros), they can take many forms and can be created by many different technologies. Not to be confused with a *Digital Signature*, which is generally a stronger cryptographic approach with more complex infrastructure requirements, and is outside the scope of this policy.

Personal Identification Number (PIN) – A secret number that a claimant memorizes and uses to authenticate his or her identity. PINs are generally only decimal digits.

Signature – A signature, whether electronic or on paper, is first and foremost a symbol that signifies intent. Thus, the definition of "signed" in the Uniform Commercial Code includes "any symbol" so long as it is "executed or adopted by a party with present intention to authenticate the writing." A signature may, for example, signify an intent to be bound to the terms of the contract, the approval of a subordinate's request for funding of a project, confirmation that a signer has read and reviewed the contents of a memo, and indication that the signer was the author of a document, or merely that the contents of a document have been shown to the signer and that he or she has had an opportunity to review them.

References

- Adapted from "Digital Signature Acceptance Policy" at https://www.sans.org/security-resources/policies/general/pdf/digital-signature-acceptance-policy
- US Federal Law – ESIGN Act - 15 US Code Chapter 96 § 7006 - https://www.law.cornell.edu/uscode/text/15/chapter-96
- Commonwealth of PA – Office of Administration ITP-SEC006 – Electronic Signature Policy
- West Chester University – Information Services & Technology ISP-INF001 - Data Classification Policy

IS&T Policy Number: ISP-SEC016

IS&T Domain: Security

UNDER REVIEW

Reviewed by: Office of Information Security, Human Resources, Business & Finance

Policy Owner: Frank Piscitello, Information Security Officer

Approved by: Approved by President & Cabinet 1/29/2018

Effective Date: 1/29/2018

Next Review Date: Under Review

History:

- 12/15/2016 – Initial Draft
- 12/20/2016 – Changed references of 'digital' to 'electronic'; updated scope section
- 10/7/2017 – Proposed final draft vetted by key stakeholders to be submitted for approval.
- 12/1/2017 – Edited by VP for readability, no changes to substance
- 12/4/2017 – Presented to President and Cabinet for consideration
- 1/29/2018 – Approved by President and Cabinet

Initial Approval: 1/29/2018

Review Dates:

Amended: