Use of Electronic and Digital Signatures | **POLICY**

Implementation Date: 8 /23 /2018

Definition

In compliance with CSU Information Security Policy 8100.0, Electronic and Digital Signature, CSUSM is permitted the use of electronic and digital signatures in lieu of handwritten (wet) signatures if the signature conforms to the terms below. Business processes and applications that incorporate electronic and digital signatures may not be implemented without prior risk evaluation and approval by the Information Security Office.

Authority

CSUSM President

Scope

This policy applies to all CSUSM employees, all CSUSM business processes and technologies used to manage the distribution, collection and storage of business records.

Karen S. Haynes, President

8/23/2018
Approval Date

I. DEFINITIONS

A. Confidentiality: Only authorized people or systems can access the protected data.

B. Integrity: The assurance that the information is trustworthy and accurate, meaningful and usable.

C. Availability: A guarantee of reliable access to the information by authorized people.

D. Non-repudiation: Non-repudiation is the assurance that someone cannot deny something. Typically, non-repudiation refers to the ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated.

E. Electronic Signatures: As defined by ICSUAM 8100, an electronic signature is an electronic sound (e.g., audio files of a person's voice), symbol (e.g., a graphic representation of a person in JPEG file), or process (e.g., a procedure that conveys assent), attached to or logically associated with a record, and executed or adopted by a person with the intent to sign the record. A digitally reproduced (e.g. scanned) physical signature is a common example.

F. Digital Signatures: As defined by ICSUAM 8100, a digital signature is a specific type of electronic signature that uses cryptographic transformation of data to provide authenticity, message integrity, and non-repudiation. For a digital signature to be valid, it must be created by a technology accepted for use by the State of California and conform to technologies capable of creating digital signatures as set forth in California Government Code Section 16.5:

- It is unique to the person using it;
- It is capable of verification;
- It is under the sole control of the person using it;
- It is linked to data in such a manner that if the data are changed, the digital signature is invalidated;
- It conforms to Title 2, Division 7, Chapter 10, of the California Code of Regulations.

Digital signatures use certificates that have a public and private key. Private keys used for digital signatures are considered protected Level 1 data whose unauthorized use, access, disclosure, acquisition, modification, loss, or deletion could result in severe damaged to the CSU, its students, its employees or its customers. For the definition of the levels of data classification please review the ICSUAM standard 8065.S02-Information Security Data Classification.

II. ACCEPTABLE USES OF ELECTRONIC AND DIGITAL SIGNATURES

A. Electronic Signatures

1. Simple Electronic Signatures may convey intent of an individual to sign a record. This includes electronic forms, scanned image of handwritten signatures and

authorization by e-mail. Simple electronic signatures may be acceptable and authorized for internal CSU uses involving low risk (e.g. forms, letters, requisitions, surveys, etc.).

B. Digital Signatures
   1. Digital signatures carry a higher level of assurance as to the identity of the signer and may always be used instead of a simple electronic signature. Where not explicitly disallowed, a digital signature may be used in lieu of a wet signature. Based on risk, a digital signature may be required to provide an appropriate level of assurance as to the identities of the signers. Examples of required digital signature include but are not limited to:
      - Records or documents where the signature is required by federal law, California law, or CSU policy.
      - Whenever the level of risk from authentication errors is high (see below section Risk Evaluation).
      - All documents signed for external and high-risk internal purposes must use a digital signature method and authority approved by the Information Security Office.
   2. All documents signed for external and high-risk internal purposes must use a digital signature method and authority approved by the Information Security Office.
   3. CSUSM employees may not use self-signed certificates to digitally sign documents for high-risk documents, or documents with any third party. Please contact the Information Security Office for further information or to obtain a compliant digital certificate.

III. RISK EVALUATION

A. For any system incorporating digital or electronic signatures, an evaluation must be performed by the Information Security Office to determine risk associated with using an electronic or digital signature. The result of this assessment must be documented and included with official record of approval and any proposals submitted to the record custodian. Following are the defined levels of risk:

   - Low: The loss of confidentiality, integrity and availability could be expected to have a limited adverse effect on organizational operations, organization assets or individuals (e.g. Any internal process dealing with low dollar transaction).
   - Moderate: The loss of confidentiality, integrity and availability could be expected to have a serious adverse effect on organizational operations, organization assets or individuals (e.g. Procurements over *50,000 USD*, contract negotiations and settlements).

- High: The loss of confidentiality, integrity and availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organization assets or individuals (e.g. Processes dealing with public safety).

B. If the highest impact is "high", or there is a legal or policy mandate for a written signature then a digital signature is required.
C. If the highest impact is moderate, an electronic signature will be sufficient.
D. If the highest impact is low, an electronic signature is sufficient.

IV. MAINTENANCE AND RECORD KEEPING

A. A review of the campus electronic and digital signature standard will be conducted periodically, but no less than every three years, by the Information Security Officer. This will include an evaluation of the electronic and digital signature use and tools to determine whether any applicable legal, business, or data requirements have changed. A determination will be made as to the continued appropriateness of the risk assessment and electronic or digital signature implementation method.
B. A record of this review will be documented and filed as part of the official record for the electronic and digital signature maintained by the Information Security Office. If as a result of the periodic review the risk level changes, a new risk assessment must be completed, including review and approval.