CALIFORNIA STATE UNIVERSITY, FULLERTON

Digital and Electronic Signature Guideline

I. Purpose

As processes that were previously conducted using paper are moved to electronic forms and workflows, a mechanism for validating and identifying appropriate electronic or digital signature methods, based on risk, is required.

Definition of a Digital Signature – A digital signature is a specific type of electronic signature that uses cryptographic transformation of data to provide authenticity, message integrity, and non-repudiation. Please reference ICSUAM 8100 section 2 as well as CSU 8100.S01 Digital and Electronic Standards for additional information and requirements.

Definition of Electronic Signature – 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.

Definition of electronic acknowledgement - Electronic acknowledgement requires the lowest level of authenticity. This form of acknowledgement is commonly used in systems with acceptance or "approve" checkboxes. Electronic acknowledgement based mechanisms rely on software configuration safeguards to provide authenticity. For instance, login banners or usage agreements that require an action every time prior to the completion of the task may be considered electronic acknowledgements because the system will not proceed to the next step without user acknowledgement

The purpose of this guideline is to provide campus continuity with the CSU Electronic and Digital Signature Policy 8100.0 and CSU Electronic and Digital Signature Standards and Procedures, 8100.S01. This guideline is to allow for Electronic or Digital Signature use at CSU Fullerton by means and methods that are practical, secure, and balance risk and cost. It is not the intent to eliminate all risk but rather to provide a process that gives parties assurance that appropriate analysis was completed prior to implementation of Electronic or Digital Signatures, and that the level of user authentication used is reasonable for the type of transaction conducted.

This guideline is meant to supply additional guidance for CSU Fullerton Administrators who have implemented or will be implementing electronic signature processes for conducting University business.

Has been approved by
Vice President Administration and Finance / CFO
Danny Kim

II. Background Information

The Federal Electronic Signatures in Global and National Commerce Act (Public Law No: 106-229) went into effect on October 1, 2000 and gives electronic contracts the same weight as those executed on paper. The act has some specific exemptions or preemptions. Any number of methods is acceptable under the act. Methods may include simply pressing an *I Accept* button, use of digital certificates, smart cards, and biometrics. Computer generated signatures may be implemented using various methodologies depending on the risks associated with the transaction.

The CSU Electronic and Digital Signature Policy 8100.0 permits the use of electronic or digital signatures in lieu of handwritten; (Wet); signatures. Usage of electronic or digital signatures is at the option of an individual campus or the Chancellor's Office provided they conform to the terms set forth.

Refer to the CSU Electronic and Digital Signature Policy 8100.0 and CSU Electronic and Digital Signature Standards and Procedures 8100.S01for appropriate definitions of terms used in this guideline.

III. Evaluation Process

Any University transaction enabled by e-signatures must be evaluated by the Units functional owner of the specific form process. For risk assessment and review purposes, similar types of transactions may be grouped together under one agreement. Implemented e-signatures will be reviewed periodically for appropriateness, and continued applicability.

An Evaluation of Risk will be performed by the Unit to determine risks associated with using an e-signature and to determine the quality and security of the e-signature method required. Please review section 6.0 of the CSU Electronic and Digital Signature Standards and Procedures, 8100.S01 document.

Determination of Electronic Signature Methodology should be commensurate to the assurances needed for the risks identified. In addition, specifications for recording, documenting, and/or auditing the e-signature as required for non-repudiation and other legal requirements shall also be determined by the Unit.

Has been approved by
Vice President Administration and Finance / CFO
Danny Kim

Units that propose e-signature methods that are at a higher or lower level of assurance than indicated in the risk assessment process shall:

- Describe the reason for variance.
- Identify the potential risk of using a tool from a lower (or higher) assurance level than the risk assessment identifies.
- Identify the steps that will be taken to mitigate the risk or justify why a higher assurance level method is appropriate.
- Obtain the signed approval of the Unit director. The signed document shall be included as part of the official record for this e-signature implementation.

IV. Approval

The Unit will seek approval to implement an e-signature from the applicable records custodian, the functional owner of the process and the campus Information Security Officer, using the Proposal for Use of e-Signature form (see Addendum). It is the records custodian's responsibility to ensure that the proposed e-signature and method meet the requirements of CSU policy. In determining whether to approve an e-signature method, consideration will be given to the systems and procedures associated with using that electronic signature, and whether the use of the electronic signature is at least as reliable as the existing method being used.

Should it be deemed necessary by the records custodian, he/she will seek approval from University Legal Counsel and the appropriate information technology office or Information Security Officer (ISO).

V. Implementation

The implementation process will likely differ for each transaction and for each Unit, as it is dependent on many factors such as technical environment, appropriate assurance level, and the nature of the transaction.

VI. Maintenance and Review Requirements

Recordkeeping - A formal record of the risk assessment evaluation, e-signature method selection, and justification will be maintained by the Unit. At

such time as the University has implemented a technology security plan and infrastructure, a copy would also be filed at the office of the CISO.

Security - Software and/or hardware that is required for e-signatures, such as Public Key Infrastructure (PKI) certificates, “fobs”, or “dongle”s, will be provided by the Unit. The Unit will also ensure that appropriate controls and monitoring of the software/hardware are in place.

Periodic Review - A review of each e-signature implementation will be conducted periodically, but no less than every three years, by the Unit. This will include an evaluation of the e-signature use 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 e-signature implementation method.

A record of this review will be documented and filed as part of the official record for this e-signature implementation maintained by the Unit. If as a result of the periodic review the risk level changes, a new risk assessment must be completed, including review and approval.

Digital and Electronic Signature Guideline

Has been approved by
Vice President Administration and Finance / CFO
Danny Kim

Has been approved by
Vice President Administration and Finance / CFO
Danny Kim