

Electronic and Digital Signature Guideline
CSU Monterey Bay
Authority: Vice President for Administration and Finance/CFO

Implementation Date: January 2, 2020

Purpose

Recognizing organizations are increasingly moving away from wet ink signed paper documents for sustainability purposes and increased efficiency, it is the policy of the CSU to permit the use of electronic or digital signatures in lieu of handwritten signatures at the discretion of an individual campus provided they conform to the terms set forth in CSU Electronic and Digital Signature Policy [ICSUAM 8100.0](#), and the CSU Electronic and Digital Standards and Procedures [8100.S01](#).

Under this guideline, units within CSU Monterey Bay are authorized to use electronic and/or digital signatures that conform with ICSUAM 8100.0 and CSU Electronic and Digital Standards and Procedures 8100.S01.

Definitions

An **electronic signature** can be a sound, symbol, graphic representation, or process attached to or associated with a record and executed or adopted by a person with the intent to sign the record. A digitally reproduced (scanned) physical signature is a common example.

A **digital signature** is the cryptographic transformation of data, which when added to a message, allows the recipient to verify the signer and whether the initial message has been altered or the signature forged since the transformation was made. A digital signature is an electronic identifier, created by a computer, intended by the party using it to have the same force and effect as the use of a handwritten signature. DocuSign and AdobeSign are examples of software to enable compliant digital signatures.

At CSUMB, e-signature is the legally binding record and the digital signature is the underlying technology that helps verify the authenticity of the transaction.

Evaluation Process

For any business process incorporating electronic or digital signatures, an evaluation must be performed by the operational unit to determine risks associated with using an electronic or digital signature. Please refer to 8100.S01. Both the risk assessment and signature method determination must be documented by submitting a service ticket. The use of digital signatures must be approved by the Digital Signature Review Group prior to implementation.

Digital Signature Review Group

The Digital Signature Review Group (DSRG) is comprised of the Director of Business and Support Services, the Director of Environmental Health, Safety and Risk Management, and the campus Information Security Officer. The DSRG will evaluate requests for digital signature use, perform a risk assessment consistent with CSU policy, and respond with a decision. The DSRG will also be responsible for periodic review of digital signature implementations, no less than every three years.