Administration and Finance
Operations Detail: Financial Services - 02

Electronic and Digital Signatures
June 30, 2022

1.0 PURPOSE

This document defines the requirements for, and acceptable usage of, digital and electronic signatures at Cal Poly Pomona (CPP).

2.0 BACKGROUND

The California State University (CSU) manages and protects the confidentiality, integrity, and availability of CSU information assets and establishes procedures that define the organizational scope of the CSU information security program.

Electronic Signatures may be used for bilateral contractual and legal documents, unilateral contracts and other University controlled documents, internal campus and Chancellor's Office forms and approvals, and external forms and approvals.

Digital Signatures may be used for any record or document when permitted and unless a handwritten signature is explicitly required. Digital signatures must be used in lieu of a simple electronic signature when legally required. 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.

3.0 OVERVIEW

It is the policy of the CSU to permit the use of electronic or digital signatures in lieu of handwritten signatures. Usage of electronic or digital signatures is at the option of the campus or the Chancellor's Office provided the local policies and procedures conform to the terms set forth in this policy.

This Operations Detail and the CSU Policy does not pertain to facsimile signatures printed on checks issued by the CSU.

This Operations Detail provides guidance to the CPP campus community on the use of digital or electronic signatures for university business transactions, including, but not limited to, contracts, agreements, requisitions, invoices, internal business documents, etc. These guidelines describe the recommended practices when using a digital or electronic signature for university business and authorizes departments within CPP to use digital and/or electronic signatures in compliance with CSU Information Security Policy and Standards.

4.0 CITATIONS

CSU Information Security Policy and Standards

CPP Appropriate Use Policy

CPP Identity Assurance

5.0 PROCEDURES

CPP is permitted to use digital and electronic signatures in lieu of handwritten signatures provided they conform to the provisions set forth in these guidelines.

Per the CSU Information Security Policy and Standards, campuses must take a risk-based approach for determining the appropriate digital or electronic signature type. The campus uses the following identity assurance levels for electronic and digital signatures:

- Level 1 identity assurance: Little or no confidence in the asserted identity's validity.
- Level 2 identity assurance: Some confidence in the asserted identity's validity.
- Level 3 identity assurance: High confidence in the asserted identity's validity.
- Level 4 identity assurance: Very high confidence in the asserted identity's validity.

The assurance levels consider six areas for potential risk:

- Inconvenience, distress, damage to standing or reputation
- Financial loss or agency liability
- Harm to agency programs or public interests
- Unauthorized release of sensitive information
- Personal safety
- Civil or criminal violations

Risk Considerations	Risk Assessment			
	1	2	3	4
Inconvenience, distress, or damage to standing or reputation	L	M	M	H
Financial loss or agency liability	L	M	M	H
Harm to agency programs or public interests		L	M	H
Unauthorized release of sensitive information		L	M	H
Personal Safety			L	M-H
Civil or criminal violations		L	M	H

Based on the assessed level of risk, unless a handwritten signature is explicitly required, the following business transaction types are authorized to use a digital and/or electronic signature:

Electronic Authorizations

1. Level 1 Identity Assurance – Low Risk: Acknowledgements via email or campus forms where identity can be assured via campus single sign-on.
    a. Departments can determine what method of acknowledgement and authorization they would accept.

Electronic Signatures

1. Level 2 Identity Assurance – Low to Moderate Risk
    a. Internal (Campus) forms with approvals: Campus processes which require campus personnel to sign (e.g., PeopleSoft access form, hospitality expense approval forms, etc.) and are retained by campus personnel utilize an electronic signature. Includes internal forms and documents with validation through campus single sign on, which do not require a digital signature.
        i. Certain internal documents and forms may be classified differently, therefore, departments accepting documents may choose to accept or deny electronic signatures at their discretion, based on level of risk.

b. External forms and approvals: Processes soliciting non-protected or non-sensitive information for data gathering purposes not intended to form a contract may utilize an electronic signature (e.g., vendor confidentiality form, liability waiver).

2. Level 3 Identity Assurance – Moderate Risk
    a. Unilateral contracts and other campus-controlled documents: Processes which are signed by university personnel only may utilize electronic signatures (e.g., purchase order, etc.). Typically, these documents are intended to form a contract and are sent to an outside person or agency. Other documents where the University is the only signatory and is providing acknowledgements or approvals, an electronic signature may be appropriate.

Digital Signatures

1. Level 4 Identity Assurance – High Risk
    a. Bilateral contracts and legally binding documents: Processes creating a legally binding agreement/contract may utilize either an electronic or digital signature (e.g., elevator service contract, internship agreement, etc.). However, when the level of risk is assessed to be high (Level 4) for a particular transaction in this category, the use of digital signatures is **required**.

Technologies & Tools

CPP Division of Information Technology & Institutional Planning (IT&IP) is responsible for establishing standards and procedures for technologies and tools to support electronic signatures and digital signatures that meet Levels 1, 2, and 3 risk assessment, as well as Level 4 identity assurance documents. Technologies and tools to support the use of digital and electronic signatures are reviewed for compliance via the campus ATI/IT Review process before use.

The current list of approved electronic and digital signature technologies is provided on the IT Services website, at: https://www.cpp.edu/it/services.shtml. Refer to web page for examples.

6.0 DEFINITIONS

Electronic Authorization: The use of electronic messages sent over a telecommunications network to signify authorization or approval. *Note: Email is not a secured method for sending Level 1 data. When Level 1 data is transmitted*

electronically, it must be sent via a method that uses strong encryption per the CPP Encryption Standard.

Electronic Signature: 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. An example of this would be a digitally reproduced, or scanned, physical signature.

Digital Signature: 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:

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

7.0 CONTACTS

Michelle Cardona
Associate Vice President
Financial Services
Division of Administrative Affairs
mdcardona@cpp.edu

Carol Gonzales
AVP IT Security & Compliance/CISO
Division of IT & IP
ciso@cpp.edu

8. REVISION TRACKING

Revision History

Revision Date	Revised by	Summary of Revision	Section(s) Revised
08/04/2022	Michelle Cardona Carol Gonzales	Initial Draft	All

Review/Approval History

Approval Date	Approved by	Summary of Approval	Section(s) Approved
08/04/2022	Ysabel Trinidad John McGuthry	Initial Draft	All