CSU Dominguez Hills Administrative Policy
E-Signature Requirements

I. Purpose

As processes previously conducted using paper move to electronic forms and workflow, a mechanism for identifying the appropriate type of electronic or digital signature (e-signature) method is required. This policy is intended to supply guidance to CSU, Dominguez Hills managers regarding e-signature implementation considerations and requirements.

E-signature may be used at CSU, Dominguez Hills after a determination by the functional/process owner of a process or form and the University Information Security Officer of the most appropriate mechanism to be use based on an assessment of risk and in compliance with the CSU Electronic and Digital Signature Policy (ICSUAM 8100.0) and CSU Electronic and Digital Signature Standards and Procedures (ICSUAM 8100.S01).

The objective is not to eliminate all risk but rather to provide a process that provides assurance of appropriate analysis was completed prior to implementation of e-signatures and the level of authentication is reasonable for the type of transaction.

II. Definitions and Acceptable Use

Digital Signature – a specific type of electronic signature that uses cryptographic transformation of data to provide authenticity, message integrity, and non-repudiation.

Digital Signatures may be used where simple electronic signatures are not acceptable or authorized for use. They may be permitted or required for any record or document where a signature is required by Federal law, California Law, or CSU policy unless a hand written signature is explicitly required. A digital signature must be used instead of a simple electronic signature when legally required or when greater risks exists. See ICSUAM 8100 Electronic and Digital Signatures for additional information and requirements.

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. Simple Electronic Signatures may convey intent of an individual to sign a record and are often easier to implement. Simple Electronic Signatures may be acceptable and authorized for internal campus use involving low risk

Electronic Acknowledgement - commonly used in systems with acceptance or "approve" check boxes. Electronic acknowledgement based mechanisms rely on software configuration safeguards to provide authenticity. For instance, 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 acknowledgement. Electronic acknowledgement is the lowest level of authenticity.

Functional/Process Owner – appropriate administrator who has ultimate responsibility for defining steps in a process, approval levels required, etc. and the ability to make changes to the process, if necessary

III. Risk Assessment

University transactions enabled by e-signatures must be evaluated by the Associate Vice President or Dean responsible for the process or form to determine risks associated with using an e-signature. Determination on e-signature methodology must be commensurate to the level of risks identified. Both the risk assessment and e-signature method determination must be documented using an e-signature assessment form developed by the University Information Security Officer (ISO) and approval by the ISO is required prior to e-signature implementation. A record of the risk assessment and e-signature methodology determination shall be maintained by the respective Dean or Associate Vice President and by the ISO.

IV. E-Signature Methodology Determination

In determining 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 in use. Deans and Associate Vice Presidents may consult with Information Technology regarding system technical architecture and capacity and with University legal counsel on risk assessment determinations, as necessary.

The electronic signature type selected should be commensurate to the assurances needed to mitigate the identified risks. The lowest cost and least complex method for mitigating risk are generally acceptable. The highest impact as determined by a risk assessment should be used to select a methodology:

- A legal or policy mandate for a written signature or a risk assessment determination of high impact requires a digital signature.
- If the highest impact value is moderate, then an electronic approval will be sufficient.
- If the highest impact value is low, an electronic acknowledgement will be sufficient.

Recommendations for use of electronic signature methods at a lower level of assurance than indicated by the risk assessment process shall:

- Describe the reason for variance
- Identify the potential risk of using a tool from a lower assurance level than the risk assessment identifies
- Justify why a lower assurance level method is appropriate
- Identify the steps that will be taken to mitigate the risk
- Obtain the signed approval of the respective Vice President and include this with the official record approving use of an electronic signature method.

Software and/or hardware required for e-signatures, such as Public Key Infrastructure (PKI) certificates, “fobs”, or “dongle’s, and appropriate controls and monitoring of software/hardware are the responsibility of the respective department.

The functional/process owner also must review use of e-signatures periodically, but not less than every three years. This evaluation shall include an evaluation of the e-signature mechanism to determine whether any applicable legal, business, or data requirements have changed and a determination as to the continued appropriateness of the e-signature mechanism utilized. A record of this review must be documented and maintained in department files. If as a result of a periodic review the manager determines the level of risk has changed, a new risk assessment must be completed, including review and approval by the ISO.

Following approval, e-signature implementation will be determined based on the e-signature methodology selected, the nature of the process or transaction, and the technical environment.

The presence of an e-signature does not mean a record was properly signed or the signatory was authorized. University procedures must identify the person by position who is authorized to sign, approve, and/or prevent unauthorized actions as a result of an electronic signature.

Approved: Naomi Goodwin, Vice President, Administration and Finance
Date: June 22, 2018