CCS Administrative Procedure
8.05.01-A Electronic Signatures

Implementing Board Policy 8.05.01
Contact: Chief Information Officer, 509-279-6062

1.0 Purpose

This procedure is intended to promote efficiency, save resources, and provide parameters for the use of electronic signatures in Community Colleges of Spokane (CCS) transactions.
This procedure outlines how CCS will designate transactions for which electronic signatures will be required and recognized by CCS.

Employees must have delegated signature authority in order to execute legal documents on behalf of CCS.

2.0 Definitions

"Agreement" means the bargain of the parties in fact, as found in their language or inferred from other circumstances and from rules, regulations, and procedures given the effect of agreements under laws otherwise applicable to a particular transaction.
"Electronic" means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities, including without limitation blockchain and distributed ledger technology.

"Electronic signature" means an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with intent to sign the record.
"Electronic record" means a record created, generated, sent, communicated, received, or stored by electronic means.

3.0 Procedure for Approval and Electronic Signature Uses

Before a department can use an electronic signature method in place of a paper-based signature, such use must be authorized by the CCS Cabinet in accordance with the following process:

3.1 Department Level Risk Assessment

3.1.1 If a department wishes to use a non-paper-based signature for an agreement, it must first conduct a department-level risk assessment. The assessment is intended to ascertain the benefits associated with using an electronic signature compared to the risks associated with such use. The assessment should also identify the quality and security of the electronic signature method required as it relates to operational and legal risk. The department must document its analysis and submit a request to the Information Technology Governance and Advisory Counsel for review and recommendation to the CCS Cabinet.

3.1.2 In conducting the risk analysis, the focus should be identifying risk factors that could lead to a challenge to the validity or enforceability of the electronic signature. Guidelines for conducting this analysis are provided in the next section.

3.2 **Risk Analysis Factors** – The following analysis is a guide to how high or low risk transactions could be:

3.2.1 **Parties to the transaction** – Generally, the closer the relationship, the lower the risk of repudiation. Individual departments should consider whether the proposed transaction is:

3.2.1.1 A transaction between CCS departments or employees;

3.2.1.2 An inter-agency transaction;

3.2.1.3 A transaction between CCS and an outside, nongovernmental entity;

3.2.1.4 CCS and an individual; or

3.2.1.5 CCS and a foreign government or organization.

3.2.2 **Nature of the Relationship and Frequency of Transactions** – Risks tend to be lower when there is an ongoing relationship and when they engage in frequent transactions. On the other hand, typically the highest risk usually involves a one-time transaction between a person and an agency that has financial or legal implications. Departments should consider whether the transaction involves:

3.2.2.1 An ongoing relationship;

3.2.2.2 A new relationship with a known party;

3.2.2.3 A new relationship with an unknown party; or

3.2.2.4 An in-person signing or remote signing.

3.2.3 **The Value or Significance of the Transaction** – Departments should consider the relative value of the type of transaction against the costs associated with implementing technology and management security controls to mitigate risk. Higher risks include:

3.2.3.1 Transactions involving transfer of funds;

3.2.3.2 Transactions where parties are committing to actions or contracts that could give rise to legal or financial liability; and/or

3.2.3.3 Transactions with information protected under state or federal law such as where the party is fulfilling a legal responsibility, which if not performed creates a legal liability or where the party is certifying information, which if not true creates a legal liability.

3.2.4 **The Risk of Unauthorized Alteration or Other Compromise** – This risk increases with the likelihood of a security intrusion to the stored record. The likelihood depends on the potential attacker's knowledge that the transaction will occur and value of information. The following transactions are higher risk:

3.2.4.1 Regular or periodic transactions between parties;

3.2.4.2 The value of information to outside parties can determine the motivation to compromise the information; and

3.2.4.3 Transactions with certain agencies who have a perceived image or mission that could warrant higher risk of attacks.

3.2.5 **Whether the Lack of a Signature Invalidates the Transaction** – The final overarching factor to consider is the extent of resulting loss or impact. If the signature is required by law then any challenge to the enforceability of the signature will usually invalidate the entire transaction. If the signature is not required but only desired, then the transaction will most likely remain valid without a signature. In addition, some transactions require a provable, electronically signed record that can be produced in case of an audit,

investigation, dispute, or litigation. Departments must consider the impact an invalidated agreement would have on operations.

3.3 Information Technology Governance and Advisory Council (ITGAC) Review and Recommendation

3.3.1 After completing the risk analysis described above, the department must submit the request to the ITGAC for review. The department should also identify the type of approved signature method that it wishes to use.

3.3.2 The ITGAC will draft guidance and provide recommendations to the CCS Chancellor's Cabinet for review and approval.

3.3.3 The ITGAC reviews information and makes recommendations in the following areas:

3.3.3.1 **IT**. Information technology staff consulted for both knowledge and guidance on the selection of a particular technology, and for a thorough understanding of existing technology architecture of the CCS District.

3.3.3.2 **IT Security**. Providing IT security knowledge and expertise to ensure adequate safeguards to protect non-public agency information.

3.3.3.3 **Business Office**. Will determine whether it makes business sense to adopt the use of electronic signatures for a particular transaction. Provides an understanding of existing processes and anticipated benefits of using electronic signatures. The business office includes Finance and Procurement, supporting the goals of the organization.

3.3.3.4 **Records Management**. Staff with knowledge of agency record retention and documentation requirements to ensure compliance with guidelines and other relevant records rules.

3.3.3.5 **Faculty and Staff**. Operational users of electronic signatures providing business case analysis and review.

3.4 CCS Cabinet Decision

3.4.1 The CCS Cabinet will review the department request and the ITGAC recommendation to use an electronic signature in place of a paper-based signature. The CCS Cabinet will go through the ITGAC risk management analysis set forth in section 3.2. In addition to assessing the level of risk to the department, the CCS Cabinet is responsible for assessing the level of risk to CCS if an electronic signature method is used and to determine if there are mitigating measures that can be used, such as using a more secure electronic signature method. The CCS Cabinet is also responsible for determining whether the department has the capabilities in place to properly maintain electronic signatures in compliance with section 5.0 of this procedure and state law.

3.4.2 After completing the risk analysis review, the CCS CIO will send the department a memo approving or disapproving the request. The CCS Cabinet may also place parameters over the use of such signatures or permit them for a limited period of time to test a certain method.

3.5 Periodic Review

3.5.1 A review of each electronic signature implementation will be conducted periodically, but no less than every time an approach or solution changes by the

department and CCS Cabinet. This will include an evaluation of the electronic signature used 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 signature implementation method.

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

4.0 Procedure for Approving Electronic Signature Methods

4.1 There are many different methods of electronic signatures. Any electronic signature method approved for use at CCS will conform to the Electronic Signature Guidelines established by the Office of the Chief Information Officer. Before a department is permitted to utilize electronic signatures, the particular electronic signature method must be approved for use by the CCS Cabinet. Before approving an electronic signature method, the CCS Cabinet must assess whether it meets the following criteria:

4.1.1 **Identification and Authentication of the Signer**. A signature must be the act of the specific person identified in the agreement. If the alleged signer later denies signing, the signature could be unenforceable unless there is proof the alleged signer actually signed the record. The parties relying on the terms of a signed transaction must determine the type of electronic signature that best meets the college's needs to identify and authenticate a signature based on level of business impact or loss if the alleged signer denies their involvement in the transaction.

4.1.2 **Intent to Sign**. The signing process should clearly identify the reason for signing and specify the actions to be taken by the signer to signify intent. To avoid confusion regarding a signer's intent, any method used must give the signer an opportunity to review the entire document, ensure it contains the same signature elements as it would if it were a paper record, require the signer to indicate assent to the document by clicking an accept or reject button, and record and retain a copy of the date, time and the signer's indicated intent.

4.1.3 **Association of Signature to the Record**. The electronic signature must be attached to or associated with the electronic record being signed. The data comprising the electronic signature must be saved. It is recommended that the following data be affixed with the electronic signature:

4.1.3.1 Identity of the signer;

4.1.3.2 Date and time of the signature;

4.1.3.3 Method used to sign the record; and

4.1.3.4 A reasoning for the signing.

Whichever method is used to associate the signature with the document, it is imperative that the college obtain and maintain proof that a specific electronic signature was applied to or used in connection with a specific electronic record.

4.1.4 **Integrity of the Signed Record**. The integrity of the document relies on the ability of the storage process used to protect it from unauthorized persons and natural disasters. Steps must be taken to preserve the accuracy and completeness of the electronic information. Further measures should be taken to

ensure no unauthorized alterations are made to the document. This protection is possible through the system that manages the electronic record. This system must ensure that a record, its signature, any associated data or links cannot be tampered with or modified.

If the electronic signature is being used for interstate transactions or for documents required by the federal government, it must meet all of the requirements of the Electronic Signatures in Global and National Commerce Act (E-SIGN), 15 USC § 7001-7031.

4.2 **Approved Electronic Signature Methods**

4.2.1 The approval of an electronic signature method can limit the use of that method to particular electronic records, particular classes of electronic records, or particular college departments.

4.2.2 Types of electronic signature methods that may be considered include:

4.2.2.1 **Click Through or Click Wrap** - This method has a signer affirm his or her intent by clicking a button. Some versions require signers to type their name, some personal identifier or type “I agree” before clicking a button. These types of electronic signature should only be used for low-risk, low-value transactions.

4.2.2.2 **Personal Identification Number (PIN) or Password** - This method requires a person to enter identifying information such as a PIN or password and the system verifying that the PIN or password is associated with the person accessing the system to authenticate the person. Examples would include requiring a student to type in a student identification number. This method is more secure than a click through agreement, but less secure than a digitized or digital signature because someone other than the person identified in the agreement could have obtained the other person’s PIN or password.

4.2.2.3 **Digitized Signature** - This method is an image of a handwritten signature. It is most effective if applied at the time of signing and can be compared to copies of digitized signatures on file. If special software judges the two images comparable, the signature is deemed valid.

4.2.2.4 **Digital Signature** - This method is created when the signer uses his or her private signing key to create a unique mark on an electronic document. The recipient of the document employs the signer’s public key to validate the authenticity of the private key to verify the document was not altered after signing. If approved electronic signature methods require the use of encryption technology that uses public or private key infrastructure and/or certificates, Information Technology will be responsible for the administration of such public or private keys and certificates.

4.2.2.5 **Hybrid Approaches** – Hybrid electronic signature solutions are available by combining techniques from various approaches to provide increased security, authentication, record integrity, and non-repudiation.

4.3 **Repealing an Approved Method**

4.3.1 In the event that it is determined that an approved electronic signature method is no longer meeting college needs, the CCS Cabinet may revoke the approval of that electronic signature method. In the event authorization of a method is

revoked, the college will take steps to minimize the risk, such as having people re-sign documents with an approved signature method.

5.0 Preserving Electronic Agreements and Signatures

5.1 Preserving the electronic document is a necessary step in the electronic records process. Electronic records must be retained for the same length of time as if it were signed in ink. Retention of the record means it needs to remain usable, searchable, retrievable and authentic for the entire length of time it must be preserved. For an electronic signature, the record must include; what the signer is agreeing to, the signature, date and time of the signing and evidence of the process the person followed to establish their identity and a clear intention to sign. Electronic signatures must be displayed as close as possible to the other terms of the transaction. The more remote the signature on the display is from the other terms, the more difficult it becomes to prove intent.

5.2 Changes in technology need to be considered when retaining electronic records in the event that they need to be changed to other electronic formats.

5.3 The department also must maintain chain of custody of the record, including employing sufficient security procedures to prevent additions, modifications, or deletion of a record by unauthorized parties. If there is a break in chain of custody, it must be documented.

5.4 Printing and retaining a hard copy is not a substitute for the electronic version unless approved by the records custodian.

5.5 Additionally, a record of the risk assessment evaluation, approval from the CCS Cabinet, and electronic signature method selection must be maintained by the department.

6.0 Related Information

6.1 RCW 1.80, Uniform Electronic Transaction Act

6.2 Office of the Chief Information Officer, Electronic Signature Guidelines, v.1.0, April 2016.

Originated: October 2020
Cabinet approval: March 2021