

# Skagit Valley College

## Electronic Signature Procedures

### Summary:

Skagit Valley College encourages electronic transactions.

An electronic signature is a sound, symbol, or process attached or associated with an electronic record and executed or adopted by a person with the intent to sign the record. Signatures are used when:

- required by law and/or,
- the significance of a transaction need to be emphasized, and/or,
- the transaction needs to be bound to a person.

Signatures emphasize one or more of the following four parts:

1. the identification and authentication of the signer,
2. the intent to sign,
3. the association of the signature to the record,
4. the authenticity and integrity of the record preserved over time.

Typical electronic signature types are:

- Click Through or Click Wrap: In this approach, a signer is asked to affirm his or her intent or agreement by clicking a button. The Click Through or Click Wrap approach is commonly used for low risk, low value consumer transactions.
- Personal Identification Number (PIN) or password: When using a PIN or password for an e- signature, a person is required to enter identifying information, which may include an identification number, the person's name and a "shared secret" such as a PIN and/or password. The system checks that the PIN and/or password is in fact associated with the person accessing the system and "authenticates" the person.
- Digitized Signature: A digitized signature is a graphical image of a handwritten signature. This approach may use specialized hardware or software for additional security.
- Digital Signatures: A "digital signature", is created when the signer uses a private signing key to create a unique mark (called a "signed hash") on an electronic document. The recipient of the document uses the signer's public key to validate the authenticity of the private key and to verify that the document was not altered after signing.
- Hybrid Approaches: Hybrid electronic signature solutions are available by combining techniques from various approaches to provide increased security, authentication, record integrity and non-repudiation.

### Procedure:

Specific methods for electronic signatures may be approved on a case by case basis by the VP for Administrative Services in consultation with the Director of Information Technology (I.T.) A list of transactions so approved will be kept in the College SharePoint site, under the I.T. Department.

Transactions may be approved for electronic signatures based on the following five factors:

1. An analysis of the need for signatures.
2. An analysis of the risks inherent in the process.
3. A description of the processes and methods proposed.
4. A list of specific groups or people that can or cannot use the process and alternative opt-out procedures.
5. A description of the impact to privacy and consistency with existing privacy policy.

To request approval. Use the form provided below.

# Request for an electronic signature.

To seek approval for an electronic signature in a transaction, please answer the following 9 questions on this or a separate sheet. Thanks for your dedication to Skagit Valley College.

1. The new electronic signature would: (circle one)

- replaces an existing electronic signature
- replaces an existing hardcopy signature
- establishes a new electronic signature

2. Name of Transaction (or name of form):

3. Description of transaction (or form) including

4. Who will be signing, and who will be receiving the signature?

5. Why do you need a signature?

- Is a signature required by law? Y or N If yes, give reference here:
- Is the signature used to emphasize the significance of the transaction? Y or N
- Is the signature used to bind a person to a transaction? Y or N
- Is the signature used to establish or verify the integrity of information? Y or N
- Is the signature used to ensure that a person cannot later deny the information? Y or N
- If there are other needs for a signature, please list them here:

6. What is the overall risk of adverse effect for this transaction? (use the worksheet below.)

- Very low
- Low
- Moderate
- High
- Very high

7. How will you establish the signature?

- What sound, symbol, or process will be used as a signature on the electronic record?
- How will the process identify and authenticate of the signer?
- How does the process establish the intent to sign?
- How does the process maintain the association of the signature to the record?
- How does the process maintain the authenticity and integrity of the record over time (including consistency with existing document management requirements).
- How will the process provide for printing, downloading, and hardcopy alternatives

8. List the groups of people who will be able to use this process. Describe opt-out procedures and accessible alternatives for people with disabilities.

9. Please describe the impact to privacy and consistency with existing privacy policy.

## Sample risk analysis for electronic signatures.

A qualitative risk analysis is needed for each approved transaction. The following three step analysis does not prevent misfortune, but rather helps to orient the design and document the concerns.

### Step One: Likelihood of a challenged.

Circle the answer to each of the five questions below. The first answer in each set indicates low likelihood; the second answer in each set indicates concern; the third answer indicates high likelihood of a challenge.

What is the relationship between parties? (From the point of view of the signer.)

1. Helpful: a history of, or reason for, collaboration
2. Neutral: no previous conflicts and no expectation for collaboration
3. Adversarial: a history of, or reason for, conflict

What is the nature of the transaction? (From the point of view of the signer.)

1. Unique transaction
2. Established but infrequent
3. Established and often repeated.

What is the financial value of the transaction? (From either the point of view of the signer or the agency, whichever is greater.)

1. None
2. Less than \$1,000
3. More than \$1,000

What type of data is exchanged in the transaction?

1. No personally identifiable information.
2. Directory information but no other personally identifiable information.
3. Directory information plus other personally identifiable information.

What is the legal value of the transaction?

1. No legal liabilities in the transaction.
2. Inaccurate info would create a legal liability for one of the parties.
3. The transaction establishes a legal responsibility for one of the parties.

### Step Two: Adverse impacts from a successful challenge.

Circle the answer to each of the four questions below. The first answer in each set indicates low impact; the second answer in each set indicates moderate impact; the third answer indicates high impact.

Is the signature required by law?

1. No, the transaction remains valid and its enforceability remains unchanged without a signature.
2. No, the transaction remains valid but its enforceability is weakened without a signature.
3. Yes, the signature is required by law and a successful challenge would invalidate the entire transaction.

What is the financial impact of an unenforceable signature? (to either the signer or the agency, whichever is greater.)

1. None
2. Less than \$1,000
3. More than \$1,000

What is the non-monetary impact of an unenforceable signature? (to either the signer or the agency, whichever is greater.)

1. None
2. Moderate
3. Large

How important is a provable record at some future time?

1. We do not need the signature to last beyond the transaction.
2. We expect the signature to be useful but not necessary in the future (for research or archives for example).
3. We may need a valid signature in the future for an audit or evidence in court.

### Step Three: Overall Risk.

Risk can be expressed as likelihood multiplied by impact.

1. How many high likelihood responses (third answer) did you indicate in Step One?
  - a. If zero, enter 1
  - b. If one, enter 2
  - c. If two or more enter 3
2. How many high impact responses (third answer) did you indicate in Step Two?
  - a. If zero, enter 1
  - b. If one, enter 2
  - c. If two or more enter 3
3. Multiply the answer in Q1 times the answer in Q2
  - a. If 1 = go to question #4;
  - b. If 2 or 3 = high risk; (end of analysis, do not do Q4, Q5, or Q6)
  - c. If 4 or more = very high risk. (end of analysis, do not do Q4, Q5, or Q6)
4. How many mild likelihood responses (second answer) did you indicate in Step One?
  - a. If zero, enter 1
  - b. If one, enter 2
  - c. If two or more enter 3
5. How many mild impact responses (second answer) did you indicate in Step Two?
  - a. If zero, enter 1
  - b. If one, enter 2
  - c. If two or more enter 3
6. Multiply the answer in Q4 times the answer in Q5
  - a. If 1 = very low risk
  - b. If 2 or 3 = low risk;
  - c. If 4 or more = moderate risk.