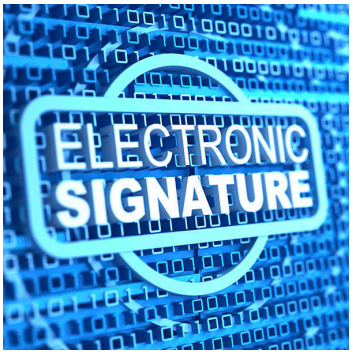
Electronic Signature Guidelines




v 1.0, April 2016

WA · Office of the
Chief Information Officer

Table of Contents

Purpose

The following individuals were members of the **Electronic Signature Workgroup** and participated as subject matter experts throughout the drafting and review of these Guidelines.

Julie Blecha, Secretary of State

Scott Bream, Washington Technology Solutions

Deborah Carr, Department of Early Learning

Cindy Cavanaugh, Department of Licensing

Johnna Craig, Office of the State Treasurer

Bruce Dempsey, Department of Health

James Gayton, Health Care Authority

John Ginther, State Board for Community and Technical Colleges

Sean Krier, Department of Health

Mark Lyon, State Office of the Attorney General

Roselyn Marcus, Office of Financial Management

Troy Niemeyer, State Auditor's Office

Wolfgang Opitz, Office of the State Treasurer

Meredithe Quinn-Loerts, Department of Social and Health Services

Becci Riley, Department of Enterprise Services

Ryan Smith, Washington Department of Veterans Affairs

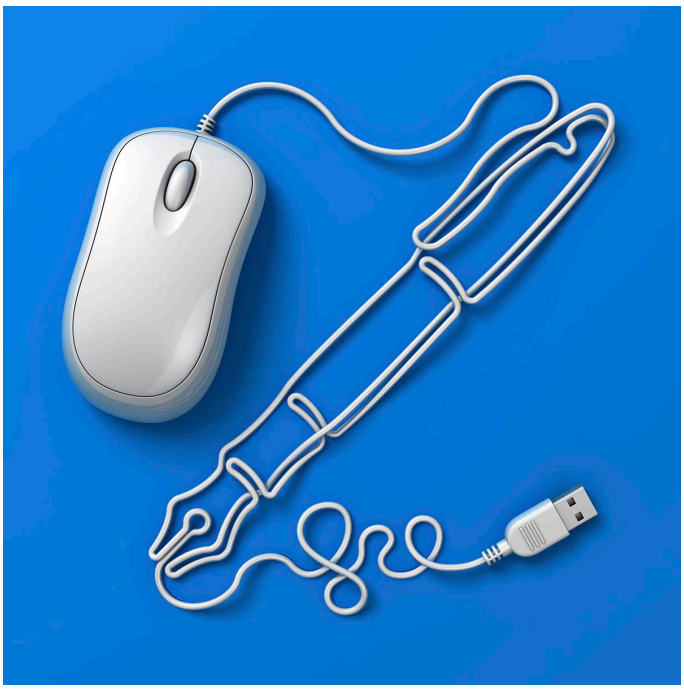
Monika Vasil, Department of Social and Health Services

Russell Wood, Secretary of State

This document provides **Electronic Signature Guidelines** for Washington state agencies to:

1. Help agencies determine if, and to what extent, their agency will implement and rely on electronic records and electronic signatures.
2. Provide agencies with information they can use to establish policy or rule governing their use and acceptance of electronic signatures.
3. Provide direction to agencies for sharing of their policies with the Office of the Chief Information Officer (OCIO) pursuant to state law.

These Electronic Signature Guidelines were developed in partnership with representatives from fourteen Washington state agencies. They are intended to be used to help state agencies best make risk-based decisions regarding electronic signatures and electronic records.



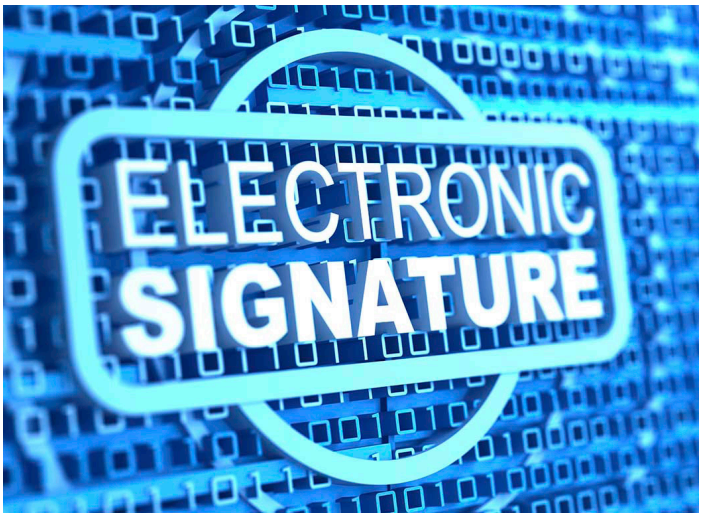
Background

The use of electronic records and electronic signatures can significantly reduce costs, simplify transactions, and speed up transaction time. Until recently there has remained some confusion under Washington law about whether state agencies can use electronic signatures to authenticate electronic transactions and what kind of technology is permissible.

The law authorizing state agencies to utilize electronic signatures in the conduct of governmental affairs and other transactions is codified in Chapter 19.360 RCW. It provides that "the legislature, to the extent not already authorized by federal or state law, authorizes electronic dealings for governmental affairs" and "intends to promote electronic transactions and remove barriers that might prevent electronic transactions with governmental entities."[1]

Unless otherwise provided by law or agency rule, state agencies may use and accept electronic signatures with the same force and effect as that of a signature affixed by hand.[2] Where a "writing" is required by statute, an electronic record may be used, and whenever the term "mail" is used,[3] the term includes the use of email or other electronic system, if authorized by an agency rule or policy.[4]

Each state agency may determine whether and to what extent it will use and rely upon electronic records and electronic signatures. Unless otherwise required by law, a state agency is not required to send or accept electronic records or electronic signatures for an agency transaction.[5]



However, there may be other state or federal laws that require use of electronic signatures or writings. Each agency will need to conduct its own evaluation of the relevant requirements. Each agency will also need to conduct its own business assessment and risk analysis of agency electronic transactions to determine if electronic signatures are appropriate, and identify the processes and technology necessary.

1 RCW 19.360.010
2 RCW 19.360.020
3 RCW 19.360.040
4 RCW 19.360.050
5 RCW 19.360.020(2)

These Guidelines

In accordance with RCW 19.360.020(4), the Washington State Chief Information Officer (CIO), in coordination with state agencies, must establish standards, guidelines, or policies for the electronic submittal and receipt of electronic signatures by state agencies, taking into account reasonable access and reliability for persons participating in governmental affairs and governmental transactions. A state agency's policy or rule on electronic submissions and signatures must be consistent with policies established by the CIO.[6]

These guidelines satisfy the statutory requirement to provide state agencies with information they may use to implement electronic signatures and engage in electronic transactions as contemplated by Chapter 19.360 RCW.

While these guidelines are being provided by the CIO, state agencies shall be ultimately responsible for determining how and when electronic signatures and electronic records will be used, and agencies shall be responsible for any liability that may result from their use.

6 RCW 19.360.020(4)

Determining the Need for a Signature

Agencies should first determine whether a signature is required or desired. When evaluating whether to use an electronic signature for a particular transaction, it is important to ask two questions:

1. Is it legally required, and/or;
2. Is an electronically signed transaction desirable.

Legal Requirement for a Signature

In many cases, a transaction is governed by a law or regulation that requires the presence of a signature before it will be considered legally effective.

As a first step, agency staff should review law(s) applicable to the transaction and determine if a signature is required. If so, conducting the transaction electronically requires an electronic signature.

Transaction-Based Need for a Signature

If there is no legal requirement for a signature on a particular type of transaction, it is recommended that agency staff undertake a further analysis to evaluate the desirability of incorporating a signature. An electronic signature may be desirable where there is a:

- **Need for Emphasizing the Significance of the Transaction.** A signature reinforces the significance of the undertaking. It gives the transaction a formal tone and drives home to the signing party the seriousness of the undertaking. In essence, it performs a cautionary function. It also gives the signing party a signal that they are entering into a legally binding transaction so the party understands the nature and importance of the transaction.
- **Need for Binding a Party to the Transaction.** If the transaction involves an intent element (e.g., agreement, approval, acknowledgment, receipt, witnessing, etc.), a signature may be useful to help formally bind a person to that reason for signing and make it more enforceable (e.g., to mitigate

concerns regarding repudiation). Likewise, where there is a risk of fraud, a signature might be useful for enforcing enhanced criminal penalties. Thus, where evidence of a party's intent is important to the transaction, a signature can provide evidence of deliberation and informed consent.

Analysis for determining whether an electronic signature is required or desired for an electronic transaction can be summarized in Table 1.

Table 1	Signature Required by Law or Regulation Governing Transaction	Signature NOT Required by Law or Regulation
There is a Need for Emphasizing the Significance of the Transaction	Electronic Signature Required	Electronic Signature Recommended
There is a Need to Bind a Party to a Specific Intent Transaction	Electronic Signature Required	Electronic Signature Recommended
All Other Transactions	Electronic Signature Required	Electronic Signature Optional or Not Needed

Definition and Characteristics of an Electronic Signature

RCW 19.360.030(2) defines an electronic signature as:

> "An electronic sound, symbol, or process, attached to or logically associated with an electronic record and executed or adopted by a person with the intent to sign the record."

This definition affords the parties to an electronic transaction the greatest possible flexibility in selecting an appropriate electronic signature solution. However, it also sets some parameters on what constitutes an electronic signature.

"An electronic sound, symbol, or process"

A wide range of digital objects may serve as an electronic signature. A digital object is any discrete set of digital data that can be individually selected and manipulated. This can include shapes, pictures, a string of numbers, or characters that appear on a display screen, as well as less tangible software artifacts. These objects can be as simple as a set of keyboarded characters or as sophisticated as an encrypted hash of a document's contents.

A process can also serve as an electronic signature. A process can create an electronic signature when a system used to create a signed e-record associates the recorded events of accessing an application with the content to be signed, thereby creating a virtual record of the signer's actions and intent. Often such signing processes also utilize a password, PIN, or other digital object for authenticating the signer.

"Attached to or logically associated with"

A penned signature becomes part of the paper document and remains with the document during transit and after it is filed. An electronic signature is considered to be "attached to or logically associated with an electronic record" if the electronic signature is linked to the record during creation, transmission and storage.

"An electronic sound, symbol, or process, attached to or logically associated with an electronic record and executed or adopted by a person with the intent to sign the record."

The linking of the e-record to an electronic signature can be achieved by various means. For instance, a digital signature, which is a kind of electronic signature, can be a discrete digital object that is embedded as part of the document in the same manner as an ink signature.

Alternatively, an electronic signature can be an object associated with the document through an embedded link. If the signing object is not embedded in the e-record, it must be maintained separately but logically associated with the record through a database, index, or other means.

When a process serves as an electronic signature, the system used to create a signed e-record logically associates all the signed record's components. An example is a document created with a person's sign-on to a procurement system, where the person has been authorized to access the system only to create a signed procurement document. In this example, the person's authority to sign is embedded in the system. The record is created through a sign-on authentication using a PIN or password and the person's subsequent actions are captured while he or she is accessing the system. The record exists conceptually as a document in the system, although the various pieces of the actual record may be maintained in various databases and system logs. The collection and maintenance of different informational pieces, also known as electronic signature "metadata," along with the person's intent to sign the record, creates an electronic signature under Washington law.

"An electronic record and"

The attachment or logical association between the signed record and the electronic signature (sound, symbol, or process), must be created at the point a record is signed, maintained during any transmission of the signed record, and retained for as long as the signed record is needed including any subsequent storage. See the Records Management section of these guidelines for information on the retention and preservation of electronically signed records.

"Executed or adopted by a person with intent to sign the record"

The essence of a signature is to identify the signer and signify that he or she understood and intended to carry out whatever was stipulated in the signed document.

Washington law does not require any specific level or method of signer identification or authentication. However, the identification and authentication methods used for a given transaction should be sufficient to support the enforceability of an electronically signed record should the alleged signer later deny they were a party to the transaction.

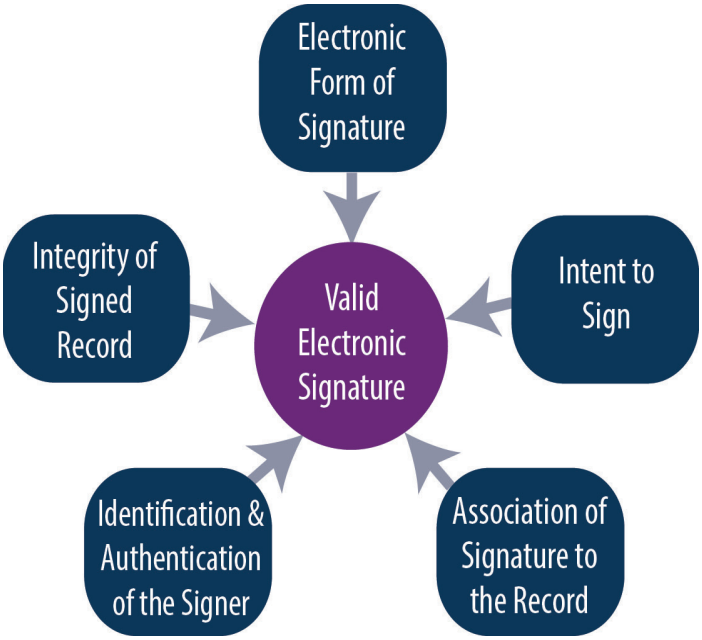
The ceremonial act of signing with pen and ink warns the signer that he or she may be making a legally binding commitment. An electronic signature must be accompanied by the same intent as the use of a signature affixed by hand.

A signer's intent can be captured in a number of ways. For example, a signer's actions can be automatically captured and recorded after entering an information system. However, to avoid any confusion as to what signers intended by their actions, it is advisable that agencies not rely solely on a signer's actions as recorded by a system to document intent. This can be done by various means, such as including a statement of intent that must be acknowledged and accepted by the signer prior to the electronic signature being applied.

As a means of further establishing intent, to the extent possible, the electronic form of signature should be displayed as close as possible to the other terms of the transaction.

Required Electronic Signature Components

Consistent with the definition of an electronic signature, in order for an electronically signed record to be deemed valid, it must satisfy five major signing requirements.



These signing requirements, taken together, need to be as reliable as appropriate to address any anticipated challenges to the enforceability of the signature.

Electronic Forms of Signature

Various methods can be used to create "an electronic sound, symbol, or process", which is one of the major components of an electronic signature. These can include a number of technologies, digital objects, or processes. The descriptions below provide information on some of the major approaches used to apply an electronic form of signature. These methods are roughly organized from the lower to the higher levels of assurance value.

- **Click Through or Click Wrap.** In this approach, a signer is asked to affirm his or her intent or agreement by clicking a button. Some Click Wrap approaches require signers to type his or her name, provide some other personal identifier, or type "I agree" before clicking a button to protect against later claims of errors. 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 accessing an application is required to enter identifying information, which may include an identification number, the person's name and a "shared secret" (called "shared" because it is known to both the user and the system), 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. Some applications require a person to create a handwritten signature using a special computer input device, such as a digital pen and pad. A digitized signature is most effective if it is applied (not copied) 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. This approach shares the same security issues as those using the PIN or password, because the digitized signature is another form of shared secret known both to the person and to the system.
- **Digital Signatures.** A "digital signature," which is a type of electronic signature, is created when the signer uses their private signing key to create a unique mark (called a "signed hash") on an electronic document. The recipient of the document employs the signer's public key to validate the authenticity of the attached

"By definition, a signature must be the act of a specific person. If the alleged signer later denies signing, the signature may be unenforceable unless there is proof the alleged signer actually signed the record."

private key and to verify that the document was not altered after signing. Digital signatures are often used within the context of a Public Key Infrastructure (PKI), in which a trusted third party known as a Certification Authority (CA) binds individuals to private keys and issues and manages certificates.

- **Hybrid Approaches.** Hybrid electronic signature solutions are available by combining techniques from various approaches to provide increased security, authentication, record integrity, and non-repudiation. For example, a solution may involve improved signature capture techniques combined with Click Wrap, PINs, and password approaches. These solutions can enhance such signatures by recording the entire transaction process, which is then bound to the signed document using hashing and SSL (Secure Socket Layer) encryption techniques to achieve document integrity and non-reputability.

Identification and Authentication of the Signer

By definition, a signature must be the act of a specific person. If the alleged signer later denies signing, the signature may be unenforceable unless there is proof the alleged signer actually signed the record.

It is up to the parties that rely on the terms of a signed transaction to determine whether the level of confidence provided by a given identification and authentication process is appropriate. The level of confidence required should be based on the level of business impact or loss that may be realized should the alleged signer later deny their involvement in the transaction.

For intra- or inter-agency transactions, the process used to verify the identity of an employee prior to assigning a login credential (user name and password) may be sufficient.

For transactions external to state government, other methods may be appropriate. In increasing levels of confidence, these may include:

- Presentation of identifying materials or documentation
- Presentation of identifying materials or documentation and follow-on verification to prove the documentation is legitimate
- In-person presentation and notarization of identifying materials or documentation

The use of third-party identity proofing services may also be used to determine identity based on scoring models used by the service.

Intent to Sign

The overall signing process should be designed to minimize the risk that signers could legitimately claim later that they applied an electronic form of signature without realizing its legal significance or their obligation to be bound by the terms of the transaction.

The overall signing process should be designed to clearly identify the reason for signing and clearly specify the actions to be taken by the signer to signify intent. Much like a signing block on a paper record, the creation of a signing ceremony in an electronic record can be used to establish intent.

A number of simple practices can help avoid confusion regarding a signer's intent:

- Prior to applying an electronic signature, afford the signer an opportunity to review the entire document or content to be signed.
- Format an electronically signed record to contain the same signature elements captured in a paper record, allowing a reader to readily identify the significance of the signature appearing on the bottom line.

"It is also recommended that..additional data elements be appended to or associated with the signature data."

- Require the signer to act affirmatively to indicate assent to the document being signed. For example, require the signer to click an "Accept" button. A button allowing the signer to "Reject" could also be presented to demonstrate that a choice was made. Alternatively, the signer could be required to type specific words of acceptance (e.g., "I ACCEPT" or "I AGREE").
- Record the date, time, and fact that the signer indicated his or her intent and retain this information for evidentiary purposes. This may be different than the time the signer accessed the application or was authenticated.
- Some electronic signature products on the market provide a "ceremony" that warns a signer that a legally binding commitment is being made, collect contextual information about the circumstances of the signing, provide formats and visual signatures similar to those found in paper documents, and collect information concerning the signer's intent.

Association of Signature to the Record

In a paper transaction, when a handwritten signature is applied, it becomes permanently affixed to the record. Likewise, for an electronic signature, the sound, symbol, or process that constitutes the signature must in some way be attached to, or associated with, the electronic record being signed.

Where the electronic form of signature consists of a symbol or a sound (such as a typed name, a digitized image of a handwritten name, a PIN, a digital signature, a voice recording, etc.), the data comprising the symbol or sound must be saved. Where the electronic form of signature consists of a process (such as clicking on an "I Agree" button), the system should be programmed so that completion of the process generates some specific data element to indicate completion of the signing process, or some other procedure (such as generation of a log record or audit trail) to record the act of signing.

It is also recommended that the following additional data elements be appended to or associated with the signature data:

- identity of the signer or a link to the source of identifying information, such as a validated UserID, assigned PIN, digital certificate, etc.;
- date and time of the signature;
- method used to sign the record; and
- an indication of the reason for signing

Associating the signature with the document can be accomplished using various approaches. The signature data can be embedded within, or directly appended to, the electronic record that was signed. Using this approach, the electronic signature becomes a part of, and is stored with, the electronic record being signed.

Alternatively, the data representing the electronic signature can be stored separately from the document being signed, so long as a demonstrably reliable and provable process is in place, such as a relational database or a digital signature algorithm, to associate the electronic signature with the electronic record.

Other approaches are also feasible. However, whatever the approach, it requires implementing an electronic recordkeeping process that, in the future, can provide evidence that a specific electronic signature was applied to or used in connection with a specific electronic record.

Integrity of the Signed Record

In the paper-based world, signed documents are often stored in a secure physical filing environment, as their usability, admissibility, and provability is based on the persistent integrity of the document itself (legibility, no indication of alteration, etc.). In this case, the integrity of the document relies on the ability of the storage process used to protect it from fire, water, and other environmental dangers, and to limit access to authorized persons.

Records Management

Likewise, the usability, admissibility, and provability of a signed electronic record requires that measures be taken to ensure the continuing integrity of the electronic record, and its association or linkage to, its electronic signature, and any associated data following completion of the signing process. This is particularly important in a digital context, where electronic records can be easily altered in a manner that is not detectable.

To preserve the integrity of a signed record, steps must be taken to preserve the accuracy and completeness of electronic information communicated over the Internet or stored in an electronic system. Further measures should be taken to ensure that no unauthorized alterations are made to information either intentionally or accidentally.

This protection can be achieved by the system that collectively manages the e-record and the associated electronic signature. In this case, key factors include the system's trustworthiness and the controls put in place to ensure that a record, its signature, any associated data, and links to any associated data, cannot be tampered with or modified. Other controls, such as the use of encrypted transport protocols, can be used to ensure that the integrity of the electronically signed record is not compromised during transmission.

Other measures, such as message hashing and encryption, can be applied to ensure the integrity of an electronically signed record. When used, these can reduce the risk of unauthorized access and provide a means of detecting whether a record has been tampered with or altered.

The use of electronic signatures raises questions about how an agency needs to manage the records (which are the evidence) of these transactions. This section provides guidance on how to manage electronic records and electronic signatures.

Preserving Electronic Records

There are four components that form the record/evidence of an electronic signature transaction:

1. Electronic document of what the person is actually agreeing to;
2. Electronic signature that was applied;
3. Date and time the signing occurred; and
4. Evidence of the process that the person followed to establish both their identify and their clear intention to sign the document.

In the paper and ink signature world, these elements are typically contained in a single record. However, with electronic signatures, these may be several different digital objects which need to remain logically linked together to form the record/evidence of the transaction.

Length of Time Records Need to be Retained

Records of a transaction that was signed electronically need to be kept for the same length of time as if the transaction was signed in ink. The retention requirements are based on the function and content of the records rather than its format.

For example, contracts need to be kept for six years after termination of the contract based on the statute of limitation for breach of contract. This applies the same regardless of whether the contract was electronically signed or signed with ink on paper.

Business Analysis and Risk Assessment

The records retention schedules for state agencies are available from the Washington State Archives website at:

http://www.sos.wa.gov/archives/recordsmanagement/state-agencies-records-retention-schedules.aspx

Preserving the Integrity and Authenticity of the Record over Time

As part of retaining the record/evidence of a transaction that includes electronic signatures for the minimum retention period outlined in the appropriate records retention schedule, the record also needs to:

> "...remain usable, searchable, retrievable and authentic for the length of the designated retention period." [7]

Records with longer retention periods may need to be migrated to other electronic formats or systems or both to continue to be usable, searchable, and retrievable as technology changes. However, careful planning will ensure that the integrity and authenticity of the record is preserved during the migration.

Preserving Electronic Records or Records of Transactions that Occurred through Electronic Means

Enterprise Content Management (ECM) systems are software tools that can enable state agencies to capture the records of electronic signature transactions, preserve them for the minimum retention periods, and maintain the logical links between the various electronic records.

In the absence of an ECM system, state agencies can still manage the records of electronic signature transactions utilizing other systems and/or a combination of policies and procedures to ensure the integrity of records are preserved and the components necessary to substantiate the validity of an electronically signed transaction remain authentic and intact.

Once it has been determined that a signature is required or desired, agencies should conduct a business analysis and risk assessment. The purpose of this assessment is to identify transaction risk factors that could contribute to the possibility of a challenge being made to the validity or enforceability of the signature. Agencies may consider including factors in addition to those identified throughout this section, depending on the agency's individual assessment and risk posture.

Agencies may or may not choose to use the model provided in this section to determine risk. Regardless of the assessment method, agencies should document the process used to determine transaction risk and maintain a copy of this document in their files for future reference.

With respect to each potential challenge to the enforceability of an electronic signature, a business analysis and risk assessment should consider:

- the likelihood of a successful challenge to the validity of the electronic signature; and
- the monetary loss, or other adverse impact, that will result from such a successful challenge to the enforceability of the electronic signature.

Because reliable data regarding the likelihood of a successful challenge to a signature may not be available, or the resulting impact of a successful challenge may not be capable of measurement in dollars, a qualitative approach should be taken with respect to the risk analysis. Using such an approach, the risk of a challenge being successful and having a significant impact is defined in more subjective and general terms such as high, moderate, and low. In this regard, qualitative analyses depend more on the expertise, experience, and good judgment of the agency managers conducting them than on quantified factors.

7 WAC 434-662-040

"One key factor in evaluating the risk that an alleged signer will repudiate or otherwise challenge the electronic signature..is the nature of the parties involved."

In determining whether a signing process is sufficiently reliable for a particular purpose, agency business assessments and risk analyses should consider, at a minimum:

- the relationships between the parties;
- the value of the transaction;
- the risk of unauthorized alteration; and
- the likely need for accessible, persuasive information regarding the transaction at some later date.

In addition, the agency should consider any other risks relevant to the particular process. Once these factors are considered separately, the agency should consider them together to evaluate the sensitivity of risk for a particular process, relative to the benefit that the process can bring.

Likelihood of a Challenge to the Signature

Parties to the Transaction

One key factor in evaluating the risk that an alleged signer will repudiate or otherwise challenge the electronic signature in a given transaction is the nature of the parties involved. Generally speaking, the closer the relationship and the more regulatory or corporately governed the parties, the lower the risk of repudiation.

For example, there is generally a very low risk of a party later repudiating the electronic signature in an inter- or intra-governmental transaction of a relatively routine nature. Similarly, transactions between a regulatory agency and a publicly traded corporation or other known entity regulated by that agency will often bear a relatively low risk of repudiation, particularly where the regulatory agency has an ongoing relationship with, and enforcement authority over, the entity. For the same reasons, risks tend to be relatively low within rulemaking contexts, as all parties can view the submissions of others so the risk of imposture is minimized.

Likewise, the more administratively governed the alleged signer, the lower the likelihood of repudiation. For example, the risk of repudiation is probably greatest with consumers, somewhat less with businesses (especially larger established businesses), and even less with other government organizations.

Thus, for purposes of the risk analysis, agency staff should consider whether the proposed transaction is:

- An intra-agency transaction
- An inter-agency transaction
- A transaction between a state organization and a non-state organization (federal, or local)
- A transaction between a state organization and a private organization – e.g., business, non-profit, association, etc.
- A transaction between a state organization and an individual
- A transaction between a state organization and a foreign government

Nature of the Relationship and Frequency of Transactions

The nature of the relationship and frequency of the transactions between the parties is also a relevant risk factor. Risks tend to be relatively low in cases where there is an ongoing relationship between the parties, particularly where they engage in frequent transactions.

Other types of transactions, such as those involving an ongoing relationship between the agency and non-governmental entities and persons, can have varying degrees of risk depending on the nature of the relationship between the parties. The same would apply in the case of those agency programs in which the ongoing relationship is between entities that are acting on behalf of the agency and such non-governmental entities and persons.

Conversely, the highest risk of fraud or repudiation might be for a one-time transaction between a person and the agency that has legal or financial implications. In all cases, the relative value of the transaction needs to be considered as well.

For purposes of the relationship and frequency risk analysis, organizations should consider whether the proposed transactions involve:

- An ongoing relationship between the parties.
- A new relationship with a known party.
- A new relationship with an unknown party.
- One-time, occasional, or frequently reoccurring transactions.
- An in-person signing or a remote signing.

Value or Significance of the Transaction

The value or significance of the transaction can have a considerable impact on the risk that an alleged signer will attempt to repudiate the signature. While value is often measured in terms of the dollar amount involved, other factors are also relevant.

Agency risk analyses should attempt to identify the relative value of the type of transaction being automated and factor that against the costs associated with implementing technological and management security controls to mitigate risk. Note that the value of the transaction depends on the perspective of the agency and the transaction partner.

The value or significance of the transaction may be higher in cases of:

- Transactions involving the transfer of funds.
- Transactions where the parties commit to actions or contracts that may give rise to financial or legal liability.

Transactions involving information protected under state or federal law (e.g., privacy, national security, otherwise sensitive, etc.) that increase the importance and value of the information involved include:

- Transactions where the party is fulfilling a legal responsibility which, if not performed, creates a legal liability (criminal or civil).
- Transactions where the party is certifying information or statements which, if not true or accurate, creates a legal liability (criminal or civil).

Risk of Unauthorized Alteration or Other Compromise

The likelihood of signature repudiation or other challenges to the enforceability of an electronic signature also increases with the likelihood of a security intrusion to the transaction or the stored record, especially if the intrusion affects the integrity of the signed record. The likelihood of such an intrusion can depend on the benefit to the potential attackers and their knowledge that the transaction will take place. For purposes of risk analysis, it should be noted that:

- Regular or periodic transactions between parties are at a higher risk than intermittent transactions because of their predictability.
- The value of the information to outside parties could also determine their motivation to compromise the information. Information unimportant to a state organization may have high value to an outside party.
- Certain agency programs, because of their perceived image or mission, may be more likely to be attacked independent of the information or transaction.

Table 2 below depicts a way to assess the likelihood of a signature being challenged based on various factors.

Table 2	**Likelihood for Each Factor:** Low (1)/Medium(2)/ High(3)	**Overall Assessed Rating:*** Low (1)/Medium(2)/ High(3)
Parties to the Transaction		
Nature of the Relationship or Frequency of Transactions		
Value/Significance of the Transaction		
Risk of Unauthorized Alteration/ Compromise		

* Overall Rating is a subjective determination based on the overall assessed rating for all factors.

Extent of Resulting Loss or Adverse Impact

Determining the likelihood of a signature repudiation or other challenges to the enforceability of an electronic signature is the first part of the risk analysis. Next, agency staff should consider the extent of any financial loss or other adverse impact flowing from a successful challenge to the validity of the electronic signature. This is generally a function of the value or significance of the record signed, as compared to its value or significance without a signature.

When evaluating such risks, staff should consult with their legal counsel about any specific legal implications due to the use of invalid electronic signatures in electronic transactions or documents in the application in question.

As with the analysis of the likelihood of a challenge to the enforceability of a signature, the analysis of the cost or impact of an unenforceable signature should result in a "Low," "Moderate," or "High" determination. Generally, the following factors should be taken into account in making that determination.

Whether Lack of Signature Invalidates Transaction

In the case of transactions where a signature is required by law, a successful challenge to the enforceability of the signature will usually invalidate the entire transaction. That is, it will convert the document into an unsigned record. The impact of this result depends in large part on the value or importance of the underlying transaction itself.

Conversely, in the case of a transaction where a signature is viewed as desirable, but is not legally required, the transaction may likely remain valid without a signature, but its enforceability may be weakened.

Thus, the impact on enforceability is generally much greater for transactions where signatures are required by law, but at the same time it is still important to consider the value or significance of the record signed and the overall transaction. It may well be that the weakened enforceability of a transaction that does not require a signature by law has a more significant impact in some cases than the complete unenforceability of other low value transactions where a signature is required by law.

Damages and Other Non-Monetary Impact

Where the lack of an enforceable signature renders the entire transaction unenforceable, or even where it merely increases the difficulty of proving a transaction, the dollar value of the transaction or the resulting damages (where calculable) should be considered. Likewise, the non-monetary impact of the failed transaction should also be considered. For many transactions, the dollar value of an unenforceable signature may not be readily calculable, yet the impact of the resulting non-enforceability or invalidity of the transaction may be significant.

Need for Provable Electronically Signed Records at a Future Time

In some paper transactions requiring a party's signature, the signature both identifies the party and establishes that party's intent to submit a truthful answer. Sometimes a notary or other third party signs as witness to the signature. When converting these types of transactions to electronic processes, the agency should ensure that the selected signing process is able to provide similar functions. Transactions that need a provable record at a later time include transactions where:

- Transaction information may later be subject to audit or compliance.
- Transaction information will be used for research, program evaluation, or other statistical analyses.
- Transaction information may later be subject to dispute:
  - by one of the parties (or alleged parties) to the transaction; or
  - by a non-party to the transaction.
- Transaction information may later be needed as proof in court or other forum.
- Transaction information will be archived later as long-term or permanently valuable records.

Table 3 below depicts a way to assess the extent of any financial loss or other adverse impact resulting from a successful challenge to the validity of the electronic signature.

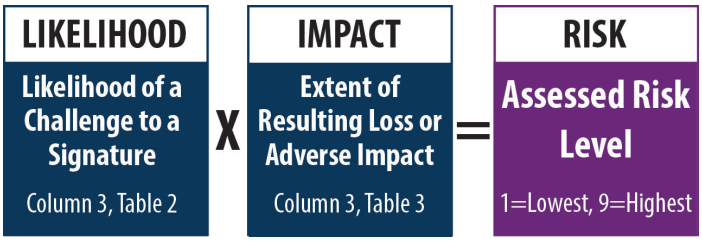
Table 3	**Impact for Each Factor:** Low (1)/Medium(2)/ High(3)	**Overall Assessed Rating:*** Low (1)/Medium(2)/ High(3)
Whether Lack of Signature Invalidates Transaction		
Damages and Other Non-Monetary Impact		
Need for Provable Electronically Signed Records at a Future Time		

* Overall Rating is a subjective determination based on the overall assessed rating for all factors.

Overall Risk Level Determination

Risk can be expressed as the product of likelihood times impact (R = L x I). Using this formula, the overall risk for a given transaction can be approximated by multiplying the Overall Assessed Rating from Table 2 with the Overall Assessed Rating from Table 3 as shown in Graphic 1 below. This will provide a relative risk rating for the transaction, with a product of "1" being low risk, and "9" representing high risk. Values in between represent proportional moderate risk.

Graphic 1: Overall Risk Level Determination



Once an agency has completed its business analysis and risk assessment, it can determine which electronic signature method or process best addresses the assessed level of risk. The strength and reliability of the electronic signature solution used should be proportionate to the level of assessed risk.

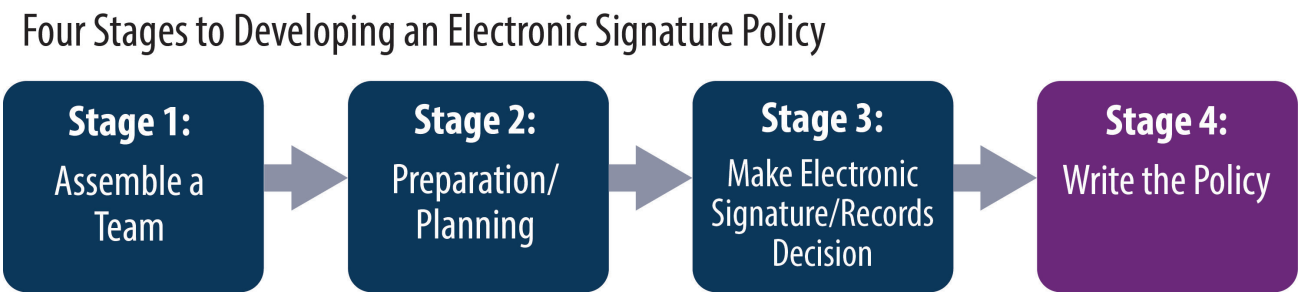
As indicated above, Chapter 19.360 RCW does not mandate that any state agency accept or require electronic signatures or records. But for state agencies that elect to do so, RCW 19.360.020(3) requires the adoption of a policy or rule establishing the "method and process" of electronic signature and record submission consistent with these guidelines.

The creation and publication of an electronic signature policy pertaining to a specific transaction or transaction type serves two primary purposes:

1. To serve as evidence that the agency has conducted a thorough analysis of the business and legal risks associated with a specific transaction or transaction type, and has documented the specific electronic signature method or processes necessary to mitigate assessed transaction risks.
2. To provide potential transaction partners with enough information to make an informed decision as to whether they can trust, and will be bound to, the methods or processes used by the agency to create and maintain electronically-signed records, and/or ensure that trading partners understand what electronic signature methods or processes are required of them when submitting electronically-signed records to the agency.

This means the agency must identify the specific electronic signature methods or processes that the agency will use or accept for a specific transaction or similar transaction types. As particular transactions are added or removed, or previously identified methods or processes change, the policy or rule should be updated so those dealing with the agency have the most current information available and can comply with the new agency protocols.

Agencies are encouraged to follow the steps listed below in order to help ensure the resulting policy or rule



meets the agency's legal obligations, business goals, and remains consistent with these guidelines and the needs of the people or entities the agency serves.

Stage 1: Assembling a Team

In order to adequately prepare for policy drafting, the agency should include a number of people from different disciplines within the agency, as there will likely be an impact on a number of different parts of the agency. As the agency moves on to information gathering, it is recommended, to the extent possible, that the areas listed below are represented.

- **IT.** Information technology staff should be identified and consulted both for knowledge and guidance on the selection of a particular technology, and also for a thorough understanding of the existing technology architecture of the organization.
- **IT Security.** The group should include someone with IT security knowledge and expertise to ensure adequate safeguards are included to protect non-public agency information.
- **Business.** The primary decision an agency will make is whether it makes business sense to adopt the use of electronic signatures or records for a particular transaction. Accordingly, knowledgeable members of the business lines impacted by any policy must be included. These members should have an understanding of existing processes and anticipated benefits of using electronic signatures or records.
- **Finance.** As agencies are being asked to engage in a cost-benefit analysis, finance personnel should be included to make sure the agency has an accurate understanding of current costs and expected savings.
- **Legal.** Either from internal or external (i.e., the Office of the Attorney General) sources, the question of whether or not a signature or record is required, and whether a proposed electronic signature solution is likely to withstand a challenge should be answered. As this will be accomplished through legal research, appropriate expertise is required.
- **Procurement.** Internal procurement staff should be included in the conversation so that they are well informed of the agency business needs and the impacts. Also, concerns discussed during the decision-making process can be well considered when determining the method of procurement and the resultant contract terms and conditions to ensure that they support the goals of the agency.
- **Public Records/Records Management.** Personnel with knowledge of agency record retention and documentation requirements should be included to ensure compliance with these guidelines and other relevant records rules.

There may be other constituencies within or outside the agency that are not a formal part of the workgroup, but may be consulted, including:

- **OCIO.** The OCIO has a central role in the adoption of electronic signatures and records by state agencies, and agencies are encouraged to take advantage of the expertise available.
- **Audit.** As discussed below, agencies may want to include audit standards in their policy. If so, audit personnel, either within the agency or at the State Auditor's office, should be consulted.
- **Communications.** As required by Chapter 19.360 RCW, the agency policy will be publicly available, and communications staff should be consulted to ensure the clarity of the final document.

Stage 2: Preparation

After the team is identified, the next step is to gather relevant information. Suggestions for additional research below include both internal and external topics. For example, existing practices and delegation of authority can be resolved internally, while information regarding available technology might require consultation with outside resources. Some areas an agency might review include:

- **Existing statutes and rules.** This work focuses on laws regarding the agency's collection and/or distribution of signatures and records. For any particular document or transaction, the first step should be to determine what the law requires the agency to do. For example, is a signature even necessary for a particular transaction? Further, the use of electronic signatures or records may be prohibited by law. Accordingly, the agency should determine whether there is any law that precludes or requires the use of electronic signatures or documents.
- **Existing agency policy and practice.** Current agency business processes should be reviewed to identify: (1) potential areas where electronic signatures and records could be effectively used, and (2) transactions and documents that are currently electronic in nature. The agency can also begin defining the requirements for those processes and determining the costs associated with each. The agency may also put this information into the agency policy as the policy is drafted.
- **Existing records requirements.** The agency will need to determine what records retention and disposition requirements apply for electronic transactions under consideration, including any retention schedule specific to the agency.
- **Technology capabilities.** The agency should have an understanding of adequate and available technological solutions, including electronic records formats and electronic signature methods related to systems currently being used by the agency. The agency should also focus on the ease-of-use of any electronic signature or records solution, considering the needs and capabilities of both end-users and agency personnel.
- **Current technological architecture.** Electronic signatures and records will also need to fit within the broader agency IT environment. In order to make an informed decision about compatibility, the agency should have a thorough understanding of its current system and where and how new electronic signatures and records can fit within it.

Stage 3: Making Electronic Signature/ Records Decision

After the agency's team has identified potential candidates for electronically signed transactions, a determination can be made whether, and in what circumstances, the agency will use or accept electronic signatures and records. For those transactions identified, the agency must adopt a rule or policy consistent with the guidelines set forth in this document.

- The agency should consider the purpose of the law: "to promote electronic transactions and remove barriers that might prevent electronic transactions with governmental agencies." Decisions made during this process should be aligned with these purposes (e.g., the agency policy should not create barriers to electronic transactions).
- Perform and document a Business Analysis and Risk Assessment similar to that described earlier, documenting the business purpose behind the decisions.

"Outside of the agency policy, the agency should consider adopting a separate policy or procedure document on how to manage implementation and maintenance of the policy."

- Determine which technologies can or cannot fit within the agency's current technological architecture. If the current architecture is a barrier to adopting a desirable technology, consider what can or should be changed within existing architecture to allow for such use.
- Begin development of instructions and training materials for end-users and agency personnel, particularly if the policy or rule will represent a substantial change in current processes or procedures.

Stage 4: Writing the Policy

The final step is to draft the agency policy reflecting the decisions made in Stage 3. RCW19.360 does not specify which electronic signature methods or processes must or should be used. Rather, those decisions are left to the agencies based on the business assessment and risk analyses they conduct. Agencies should consider the following when drafting their policy:

- The policy should clearly identify any agency-specific standards, limitations and processes, including:
  - Specific technology choices the agency has made
  - Specific transactions the agency intends to be completed electronically
  - Specific groups of constituents that can or cannot use such signatures or records (e.g., the agency allows electronic signatures for only certain contracts, or allows electronic filings only for renewal transactions but not an initial application)
  - Standard processes and methodologies the agency intends to follow or use, such as providing users with a document for printing or download as part of the signing process
  - End-user instructions and other training materials
- Agencies also need to consider developing opt-out procedures or restrictions on use, particularly when dealing directly with individual members of the public.
- If the agency elects to use electronic signatures or records in contracting, the agency should consider cross-referencing the agency's procurement policy.
- Since all such policies will be posted by the OCIO, the policy might also describe the liability and obligations of the parties to the transaction being performed electronically. The agency should also prominently display this information in appropriate places on its own website.

Outside of the agency policy, the agency should consider adopting a separate policy or procedure document on how to manage implementation and maintenance of the policy. This document may include the following:

- Identification of roles and responsibilities of agency employees in the electronic signature and record collection and review process, including who within the agency has the authority to sign documents electronically or initiate use of electronic records or correspondence.
- Procedures for changing the scope of electronic signature and record use and acceptance, including escalation and approval of any such decision.
- Electronic document retention and management practices consistent with the appropriate Secretary of State schedule and the records guidelines included in this document.

Other items for agency consideration are listed below. While these fall outside of the core purpose of the policy and relevant procedures, agencies should consider whether these should be developed in parallel with the electronic signatures and records policy.

- **Communications plan.** A good plan and timely communication with impacted parties will help provide for a smooth transition from paper to electronic modes of operation.
- **Personal Privacy Policy.** Increased use of electronic transactions may result in the (intended or unintended) gathering of additional personal or non-public information, especially for the purposes of signer authentication. The agency may want to consider developing a policy or statement indicating this possibility and outlining its statutory obligation to maintain the confidentiality of personal information in accordance with state law and rules regarding records retention and disclosure. The agency should also consider documenting how it will use this additional information, if at all.
- **Audit Policy.** As with other agency practices, consider whether a policy describing the type and frequency of internal and external audits is needed, including the agency's compliance with its policy and the accuracy of the information and records retained. This may be accomplished as an amendment to an existing policy.
- **Training Plan.** The adoption of new technologies and modes of doing business carries the potential to change an agency's processes considerably. An agency may wish to draft one or more training plans to help both internal personnel and external system users with the transition.

Submitting Your Policy to the OCIO

The Office of the Chief Information Officer maintains a page on the OCIO.wa.gov website listing links to individual agency electronic signature and record submission policies. As agencies publish their policies, the link and agency contact information should be emailed to the OCIO Policy Mailbox. The information will be added to the page within 5 working days. Agencies are responsible for notifying the OCIO if the information changes.

Attachment A
Electronic Signature Procurement Related Resources

Currently Available Applications

Depending on the business assessment and risk analysis conducted by an agency, it is possible that features and functionality that exist in currently deployed applications (such as Word, Excel, or Adobe Acrobat) may provide sufficient electronic signature capability. If so, additional procurement may not be necessary to implement electronic signatures.

Procurement of Electronic Signature Technology

If it is necessary to procure a product or service in order to meet assessed electronic signature requirements, agencies should first look to products and services offered by state central services agencies such as Washington Technology Solutions (WaTech). If none are available, check to see if a statewide Master Contract is available that meets the agency business needs. If a desired solution is not available from either of those sources, the agency may conduct its own procurement.

Central Services

Determine whether the solution is offered through WaTech. A listing of WaTech Services can be found at: http://watech.wa.gov/solutions/it-services

Master Contracts

Determine whether a statewide Master Contract is available through the Department of Enterprise Services (DES). Information on currently available Technology Master Contracts can be found at:

http://www.des.wa.gov/services/ContractingPurchasing/ITContracts/ITMasterContract/Pages/default.aspx

For questions related to specific contracts included on the website above, contact the Contract Administrator designated on the website for that contract.

Conduct a Procurement Process

If no Master Contract exists that meets your business needs, you may decide to conduct a procurement to acquire the necessary products or services. Any procurement conducted must follow procurement laws (Chapter 39.26 RCW) and policy. In addition, procurement of information technology must meet the standards set by the Office of the Chief Information Officer (OCIO).

Procurement Process

To ensure compliance with the most current DES Procurement Policies, visit: http://des.wa.gov/about/pi/ProcurementReform/Pages/Policies.aspx

Contact DES customer service at:

Phone: (360) 407-2210

E-mail: ContractingandPurchasing@des.wa.gov

To ensure compliance with the most current WaTech/OCIO technology standards, visit: https://ocio.wa.gov/

When Contracting With a Vendor for a Solution

Solution Considerations

On premise solution

The product is licensed to the agency for use in agency transactions employing electronic signatures. Documents are stored within agency technical infrastructure. Agencies should approach these procurements as they would any IT procurement/contract for products or services.

Cloud-based solution

Agencies should understand the data flow within an electronic signature process in order to determine when its data is transiting or being stored in a system other than one it controls. In the event that sensitive data flows through or is stored on a system controlled

by an entity other than the agency, appropriate security requirements, roles and responsibilities, liabilities, etc. should be included in the contract. Each agency should work with its procurement/contract professionals, Assistant Attorney General, technical staff, etc. as necessary to ensure that the data and resulting transactional documents are properly handled.

When using contractor software as a service, agencies should determine whether agency requirements for security of transactional data are being met appropriately. Agencies should require the contractor to provide proof of security policies and practices prior to using the services.

If signed documents are stored long-term (i.e., the Cloud Service is the system of record) by the contractor as a service to the agency, ensure that the systems and operational policies employed by the contractor comply with Washington state security, privacy, and records retention requirements.

If the agency's final documents will be stored on the contractor network/infrastructure, the agency should consider adding Terms and Conditions that address what happens in the event the contract for services terminates for some reason. Agencies may contact DES Contracting and Purchasing services for questions to consider when evaluating the use of software as a service.