CITY OF REDMOND
RESOLUTION NO. 1498

A RESOLUTION OF THE CITY COUNCIL OF THE CITY OF REDMOND, WASHINGTON, RATIFYING THE ADMINISTRATIVE POLICY: ELECTRONIC SIGNATURE USE

WHEREAS, Chapter 19.34 RCW, the Washington Electronic Authentication Act, grants local agencies the ability to use electronic signatures for official public business to provide reasonable assurance of the integrity, authenticity, and nonrepudiation of an electronic communication; and

WHEREAS, two types of electronic signatures are possible: 1. an "electronic signature" (an electronic sound, symbol, or process attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record (includes a "digital signature")); and 2. a "digital signature" (an electronic signature that is a transformation of a message using an asymmetric cryptosystem such that a person having the initial message and the signer's public key can accurately determine whether the transformation was created using the private key that corresponds to the signer's public key and whether the initial message has been altered since the transformation was made); and

WHEREAS, the "Intent" of RCW 19.360.020 states, "Local governments must be efficient and prudent stewards of our residents' tax resources. To best serve our communities, certain local government statutes must be amended to reflect technological and organizational change. It is the intent of the Legislature to clarify current authorities so that local government can better serve their residents, and it is the intent of the Legislature that the following sections allow local government to pursue modern methods of serving their residents while preserving the public's right to access public records, and judiciously using scare county resources to achieve maximum benefit;" and

WHEREAS, the City of Redmond is interested in updating its signature practices with respect to use and acceptance of electronic signatures for business purposes, as outlined in the policy attached (Exhibit 1) to this resolution.

NOW, THEREFORE, THE CITY COUNCIL OF THE CITY OF REDMOND, WASHINGTON, HEREBY RESOLVES AS FOLLOWS:

Section 1. Ratification of Policy. The City of Redmond Electronic Signature Policy is hereby ratified as an official policy of the City, as provided in Exhibit 1.

Section 2. Amendment of Policy. The City Council of the City of Redmond hereby acknowledges that future amendments to this

policy, if any, will be made administratively, and will be based solely on changes in law, rule, or business practice.

ADOPTED by the Redmond City Council this 1st day of May, 2018.

APPROVED:

JOHN MARCHIONE, MAYOR

ATTEST:

MICHELLE M. HART, MMC, CITY CLERK (SEAL)

FILED WITH THE CITY CLERK: April 17, 2018
PASSED BY THE CITY COUNCIL: May 1, 2018
RESOLUTION NO: 1498

YES: ANDERSON, BIRNEY, CARSON, FIELDS, MARGESON, MYERS, PADHYE

POLICY
USE OF ELECTRONIC SIGNATURES FOR CITY BUSINESS

SECTIONS

10 Electronic Signature Policy

The policy of the City is to enable employees to conduct City business through the use of electronic signatures where desired when such use is consistent with these guidelines.

20 Employee Responsibilities when Using Electronic Signatures

All City employees who utilize electronic signatures in the conduct of their duties will have reviewed these polices to ensure that, to the best of their ability, the guidelines herein are followed.

30 Authorization for the Use of Electronic Signatures

Electronic signatures consistent with this policy may be used by the City in the same way that physical signatures may be used. City staff may rely on electronic signatures which are consistent with this policy in the same way staff relies on physical signatures.

40 Definition of Electronic Signatures

Electronic signatures include an electronic sound, symbol, or process –

- A variety of digital objects may serve as an electronic signature when provided in the context as approved by the Finance Director consistent with this policy.
- The electronic signature must clearly be associated with the related paper or process intended to be attested to.
- The signature must be verifiable as part of the underlying record (e.g. a clear indication of the electronic signature must be maintained as part of the documents or process being attested to).
- The signature must have been executed or adopted by a person with an intent to sign the record as appropriate based on the nature of the document (see section 50.

50 Authorized Electronic Signatures

The Finance Director, in consultation with the City Clerk, Human Resources Director, City Attorney and Director of Technology and Information Services shall authorize acceptable forms and uses of electronic signatures.

In authorizing specific forms and uses of electronic signatures the Finance Director shall take into account the benefits as well as the risks. The following table illustrates that type of analysis that is consistent with this section.

Use Cases	Degrees of Risk				
	Very Low	Low	Medium	High	Very High
Employee Signing Timecard					
Supervisor signing personnel action notice					
Electronic purchase orders					
Class participant signing waiver					
Open bids					
Standard form contracts					
Interlocal Agreements					
Negotiated contracts					
Sealed Bids					
Real property documents					

The type of electronic signature authorized may vary relative to the nature of the risk. For example a process indicating concurrence as an electronic signature may be used for low or very low risk cases, but not for medium or high risk cases. For high risk cases, the electronic signature should take the form of a digital signature through an approved third-party process which includes verification of the specific intent to sign, an approved signature methodology, and maintenance of evidence of the electronic signature. Therefore a risk assessment of those charged with authorizing the specific forms and uses of electronic signatures should be part of the approval process.

60 Acceptable Forms of Electronic Signatures

The following electronic signature types are authorized for use:

- Very Low Risk - A process indicating approval or authorization
    1. Employee timecards
    2. Personnel action notices for performance reviews and administrative changes
    3. Performance reviews conducted with city software (NeoGov)

- Low Risk – A digital object indication approval or authorization (such as signature image)
    4. Purchase orders
    5. Personnel action notices for any action not already authorized
- Medium Risk – Use of a third-party electronic signature service (such as DocuSign)
    6. Class participant waivers
    7. Facility lease documents
    8. Open bids
    9. City standard form contracts
    10. Interlocal agreements
- High Risk – Use of a third- party electronic signature service (such as DocuSign) which has been licensed as a certification authority (CA) by the Washington Secretary of State
    11. Non-standard form contracts
- Very High Risk – Digital signatures are not authorized for very high risk use cases
    - None

80 References

RCW 19.34 - WASHINGTON ELECTRONIC AUTHENTICATION ACT
Electronic Signature Guidelines – Published by the Office of the Chief Information Officer, State of Washington
http://des.wa.gov/sites/default/files/public/documents/About/rules/ESignProcedure.pdf

Digital Signatures – Washington State Secretary of State's Office
https://www.sos.wa.gov/ea/

90 Glossary of Terms

Unless the context clearly requires otherwise, the definitions in this section apply throughout this chapter:

1. "Accept a certificate" means to manifest approval of a certificate, while knowing or having notice of its contents. Such approval may be manifested by the use of the certificate.
2. "Accept a digital signature" means to verify a digital signature or take an action in reliance on a digital signature.
3. "Certificate" means a computer-based record that:
    a. Identifies the certification authority issuing it;
    b. Names or identifies its subscriber;
    c. Contains the subscriber's public key; and
    d. Is digitally signed by the certification authority issuing it.
4. "Certification authority" means a person who issues a certificate.
5. "Certification authority disclosure record" means an online, publicly accessible record that concerns a licensed certification authority and is kept by the secretary.
6. "Certify" means to declare with reference to a certificate, with ample opportunity to reflect, and with a duty to apprise oneself of all material facts.

7. "Digital signature" means an electronic signature that is a transformation of a message using an asymmetric cryptosystem such that a person having the initial message and the signer's public key can accurately determine:
    a. Whether the transformation was created using the private key that corresponds to the signer's public key; and
    b. Whether the initial message has been altered since the transformation was made.
8. "Electronic" means electrical, digital, magnetic, optical, electromagnetic, or any other form of technology that entails capabilities similar to these technologies.
9. "Electronic record" means a record generated, communicated, received, or stored by electronic means for use in an information system or for transmission from one information system to another.
10. "Electronic signature" means a signature in electronic form attached to or logically associated with an electronic record, including but not limited to a digital signature.
11. "Hold a private key" means to be authorized to utilize a private key.
12. "Incorporate by reference" means to make one message a part of another message by identifying the message to be incorporated and expressing the intention that it be incorporated.
13. "Issue a certificate" means the acts of a certification authority in creating a certificate and notifying the subscriber listed in the certificate of the contents of the certificate.
14. "Licensed certification authority" means a certification authority to whom a license has been issued by the secretary and whose license is in effect.
15. "Message" means a digital representation of information.
16. "Private key" means the key of a key pair used to create a digital signature.
17. "Public key" means the key of a key pair used to verify a digital signature.
18. "Recipient" means a person who has received a certificate and a digital signature verifiable with reference to a public key listed in the certificate and is in a position to rely on it.
19. "Recognized repository" means a repository recognized by the secretary under RCW 19.34.400.
20. "Repository" means a system for storing and retrieving certificates and other information relevant to digital signatures.
21. "Subscriber" means a person who:
    a. Is the subject listed in a certificate;
    b. Applies for or accepts the certificate; and
    c. Holds a private key that corresponds to a public key listed in that certificate.
22. "Time stamp" means either:
    a. To append or attach a digitally signed notation indicating at least the date, time, and identity of the person appending or attaching the notation to a message, digital signature, or certificate; or
    b. The notation thus appended or attached.
23. "Valid certificate" means a certificate that:
    a. A licensed certification authority has issued;
    b. The subscriber listed in it has accepted;
    c. Has not been revoked or suspended; and
    d. Has not expired.
    e. However, a transactional certificate is a valid certificate only in relation to the digital signature incorporated in it by reference.
24. "Verify a digital signature" means, in relation to a given digital signature, message, and public key, to determine accurately that:
    a. The digital signature was created by the private key corresponding to the public key; and
    b. The message has not been altered since its digital signature was created.