ADMINISTRATIVE PROCEDURE

SECTION: 600-Information Technology	**PROCEDURE #:** 603-A
TITLE: Electronic Signature Procedure	**IMPLEMENTS POLICY #:** 603
SPONSORING DEPARTMENT/DIV: Department of Information Technology Services	
EFFECTIVE DATE: 07/10/2020	**REVIEWED:** 09/30/2024

OBJECTIVE: To establish procedures that detail when and in what form an Electronic Signature can be used by a county employee that will be accepted by Washington County and is legally binding on the County.

DEFINITIONS:

Certificate Authority (CA): Certificate Authority, or certification **authority**, is an entity that issues digital **certificates**. The digital **certificate** certifies the ownership of a public key by the named subject of the **certificate**.

Digital Signature: the process that guarantees that the contents of a message have not been altered in transit.

Electronic Signature (e-signature): the electronic process that ensures acceptance of an agreement or record.

Proof of Signing: the process of binding each digital signature to the document using encryption. This validation is performed by the Certificate Authority or Trusted Service Provider.

Public Key Infrastructure (PKI): supports the distribution and identification of **public** encryption **keys**, enabling users and computers to both securely exchange data over networks such as the Internet and verify the identity of the other party.

Service Provider: A service provider is a vendor that provides Information Technology (IT) solutions and/or services to end users and organizations.

Trusted Service Provider (TSP): a person or legal entity providing and preserving digital certificates to create and validate electronic signatures and to authenticate their signatories as well as websites in general.

AUTHORITY:
All Electronic Signature process must comply with the U.S. Electronic Signatures in Global and National Commerce Act of 2000 (ESIGN). In addition, Oregon has adopted the Uniform Electronic Transactions Act (UETA) (ORS 84.049- 84.064).

GENERAL POLICY:

County employees shall only utilize a Trusted Service Provider (TSP) approved by Information Technology Services in creating or executing documents via any Electronic Signature process.

Any Electronic Signature process used by an employee must comply with ESIGN and UETA (ORS 84.049 through 84.064). Proof of Signing must be maintained in this process, verified through audit trail. A Digital Signature is required to be applied after the Electronic Signature is provided.

PROCEDURES:

1. Information Technology Services (ITS) shall evaluate Trusted Service Providers (TSPs) and will maintain a list of TSPs approved for use. ServiceIT knowledge base article KB0013309 shows the current list of approved providers. ITS may approve additional TSPs from time to time as specific use cases are identified. Any agreement between ITS and a TSP must be administered by ITS.

2. The Digital Signature must be secured by the Service Provider using the latest encryption standard and the Public Key Infrastructure (PKI) methodology. The certificates must be issued by a Certificate Authority (CA) or Trusted Service Provider (TSP) and demonstrate the Proof of Signing to the Signed Document using the latest encryption standard.

3. County record retention policy must be adhered to for documents stored off-premise. The Service Provider shall not retain County documents and data in the event of discontinuation of business with Service Provider. The Service Provider shall provide the documents and data to the County for retention and business purposes.

4. Access to County documents and data is required to be always available from Service Provider whenever that capability is part of the service.

5. ITS shall monitor for changes to Oregon Revised Statutes and US ESIGN and revise policies and procedures as necessary.

6. Employees shall advise ITS of concerns or requests relating to e-signature technology standards through a standard service request.

7. ITS shall evaluate and review modifications to the e-signature technology.

8. ITS is responsible for taking action to assure compliance with Policy 603 as issues are identified.