City Council Policy #33
Electronic Records and Signatures

Date Approved: April 3, 2023
Dates Amended:

I. Purpose

The purpose of this policy is to establish requirements for using electronic records and electronic signatures in the transaction of official City business.

II. Scope

This policy applies to all City employees and governs the use of electronic records, signatures, and seals used to conduct official City business. Such business shall include, but not be limited to electronic communications, transactions, and other official purposes.

III. Authority

The following Federal and State laws give electronic records and signatures the same legal status as paper records and signatures:

1. Uniform Electronic Transactions Act (UETA) in Missouri (Sections 432.200 to 432.295, RSMo.) in 2003.
2. Electronic Signatures and Global National Commerce Act (E-SIGN) of 2000.
3. The State and Local Records Law (Sections 109.200 to 109.310 RSMo.).
4. Missouri Sunshine Law (Sections 610.010 to 610.310 RSMo.).
5. Missouri Code of State Regulations, Title 20 — Department of Insurance, Financial Institutions, and Professional Registration (20 CSR 2030-3.060. Licensee's Seal).

IV. Policy Statement.

1. It is the City of Kirksville's policy to use electronic records and electronic signatures as allowed by law, except where written records or signatures are expressly required; exceptions include:
    a. Contracts involving the City;
    b. Court notices and court orders;
    c. Official court documents, including briefs, pleadings, and other writings requiring execution and connection with court proceedings;
    d. Termination or cancellation of utility services;
    e. Termination or cancellation of health insurance or life insurance benefits;
    f. Documents dealing with default, acceleration, repossession, foreclosure, or eviction;
    g. Negotiable instruments and secured transactions;
    h. Wills, codicils, and testamentary trusts;
    i. Product recalls or material product failures that risk endangering health or safety; and
    j. Documents required by law to accompany transportation or handling of hazardous materials, pesticides, or other toxic or dangerous materials.
2. Use electronic seals as allowed by law, as long as they provide the ability to authenticate the document, and originator and to verify that it is unaltered.
3. Provide reasonable assurance that electronic records, electronic signatures, and associated metadata will remain accessible for full retention.
4. Recognize that there is no agreement and no contract in a contractual setting unless all parties agree that an electronic format is acceptable.
5. Insurer an electronic transaction occurs in the manner specified by law and contains any specified elements required by law.

V. Definitions

BIOMETRIC SIGNATURE: The automatic identification of a person based on their physical characteristics, such as a thumbprint or retina scan.

BIORHYTHMIC SIGNATURE: The comparison of physical signature characteristics, typically speeds and pressure of the signature, to a previously provided and stored sample.

CERTIFICATE: An electronic document attached to a public key by a trusted certificate authority provides proof that the public key belongs to a legitimate subscriber and has not been compromised.

CERTIFICATE AUTHORITY (CA): An entity that issues digital certificates to certify the ownership of a public key by the named subject of the certificate.

COMMON ELECTRONIC SIGNATURES: Any signature method that does not use a specific technology to increase the security, authenticity, or evidentiary value of a signature.

DIGITAL CERTIFICATE: A digital certificate, also known as a public key certificate, can be used to verify that a public key belongs to an individual. It is an electronic document that uses a digital signature to bind together a public key with identifying information such as the name of a person or an organization, their address, etc.

DIGITAL SIGNATURE: A specific type of electronic signature that employs signer verification and encryption technology to make it unreadable to anyone except those possessing special knowledge usually referred to as a key.

ELECTRONIC: Relates to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.

ELECTRONIC RECORD: Any information that is recorded in a form that only a computer can process and that satisfies the operative definition of "record."

ELECTRONIC SIGNATURE: Any electronic method of signing a computer-processible record.

HOLOGRAPHIC SIGNATURE: A physical likeness of an individual signature is applied electronically and bound to the content via cryptographic technology.

INTEGRITY: The integrity of a record refers to its being complete and unaltered.

METADATA: Data about the data; the description of the data resources, their characteristics, location, usage, etc. Metadata is used to identify, describe and define user data.

PUBLIC KEY INFRASTRUCTURE (PKI): PKI supports the application of digital signature technology. It is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates.

RECORD: Any document, book, paper, photograph, map, sound recording, or other material, regardless of physical form or characteristics, made or received according to law or in connection with the transaction of official business (Section 109.210.5 RSMo.).

RECORDS RETENTION SCHEDULE: A listing and description of the record series maintained by all or part of an organization, prescribing the period that each series is to be maintained after no longer needed for current business.

RETENTION PERIOD: The length of time a record series is to be kept after is no longer needed for current business.

TRANSACTION: An action or set of actions occurring between two (2) or more persons relating to the conduct of business, commercial, or governmental affairs.

VI. Roles and Responsibilities

1. Any person or entity using electronic records and signatures to conduct official City business shall:
    a. Only use electronic signatures for appropriate business purposes;
    b. Adhere to requirements set forth by the City of Kirksville;
    c. Protect and not disclose or make available their digital signature, private key, or password to other persons;
    d. Comply with requirements of professional governing boards with regards to electronic signatures, electronic seals, and electronic notarizations; and
    e. Report any suspected or fraudulent use of signatures immediately.
2. The Administrative Services Coordinator is responsible for establishing and managing a Public Key Infrastructure (PKI) and corresponding procedures.

VII. Procedure

1. The following electronic signature technologies are recognized by the City of Kirksville
    a. Common electronic signatures such as:
        i. A digital image of a handwritten signature.
        ii. A password or PIN (Personal Identification Number).
        iii. A click-through signature method accepting what is being stated onscreen.
        iv. A mark or symbol indicating intent to sign, such as /s/, indicating intent to sign.
    b. Secure Electronic Signatures, such as:
        i. Cryptography.
        ii. Biorhythmic signature.
        iii. Biometric signature.
        iv. Holographic signature.
    c. Digital signatures, which provide additional assurances and security and link an electronic document with the sign or through the use of a PKI.
2. How to choose an electronic signature:
    a. Be familiar with the City's policy and procedures for using electronic signatures, including the Electronic Records and Signature Policy
    b. Understand when electronic signatures cannot be used (see Section 155.040(A)(1) for a complete list of exceptions).
    c. Do a cost-benefit analysis to evaluate current business processes to determine if electronic signature technology is required.
    d. Do a risk assessment to help decide whether electronic signatures are feasible and, if so, what type of electronic signature is needed.
        i. Select the appropriate assurance level based on the confidence level that is required to validate the asserted identity of the electronic signature.
        ii. Determine the level of metadata required to validate the electronic signature.
    e. Consult with the IT Department for technical questions and for assistance in choosing the right PKI digital signature technology, if needed.
    f. Always protect and do not disclose or make available a digital signature private key or password to others.
    g. Notify the IT Department when individuals or entities are no longer authorized to conduct electronic business so that IT can maintain accurate revocation information.
    h. Document electronic signature processes and coordinate them with Records and Information Management (RIM) and IT Department policies and procedures.

3. Retain electronically signed records and associated metadata according to approved records retention schedules.
    a. Electronically signed records must contain the following minimum information so the entire record and associated metadata can be reproduced in an arrangement that permits the person viewing or printing it to verify:
        i. Document type (for example, MS Word 2010);
        ii. The contents of the electronic record;
        iii. The method used to sign the electronic record, if applicable;
        iv. The person(s) signing the electronic record; and
        v. The date when the signature was executed.
    b. The IT Department shall maintain the following PKI metadata and a separate database;
        i. Certificate revocation information; and
        ii. All versions of the certification practices statements.

VIII. References

1. Missouri Records Retention Policy.
2. Uniform Electronic Transactions Act (UETA) in Missouri (Sections 432.200 to 432.295 RSMo.) in 2003.
3. Electronic Signatures and Global National Commerce Act (E-SIGN) of 2000.
4. The State and Local Records Law (Sections 109.200 to 109.310 RSMo.).
5. Missouri Sunshine Law (Sections 610.010 to 610.310 RSMo.).
6. Missouri Code of State Regulations, Title 20 - Department of Insurance, Financial Institutions, and Professional Registration (20 CSR 2030-3.060. Licensee's Seal).