Electronic Delivery and Execution of Legislation and Contracts

Security and Technical Procedures

I. Purpose

The purpose of these procedures is to establish the security and technical protocols for electronic delivery and execution of legislation, contracts, agreements, instruments, and other documents in accordance with Chapter 110 of the Cuyahoga County Code and Chapter 304 of the Ohio Revised Code.

II. Scope

These procedures apply to the Department of Information Technology, the Department of Purchasing, the Fiscal Department, the County Executive, the Council President, and their respective staff members, as well as any other County personnel involved in electronic delivery and execution processes.

III. Electronic Signatures Format

1. **Electronic signature solutions**: The Department of Information Technology must select and implement secure and reliable electronic signature solutions that comply with relevant legal standards and best practices, referenced in the APPENDIX.
2. **User authentication**: The electronic signature solution must provide user authentication mechanisms, such as multi-factor authentication, to ensure that only authorized individuals can affix electronic signatures.
3. **Non-repudiation**: The electronic signature solution must provide evidence of the signer's identity and intent to sign, ensuring non-repudiation, referenced in the APPENDIX.
4. **Signature audit trail**: The electronic signature solution must maintain an audit trail of the signature process, including date and time stamps, IP addresses, and source information.

IV. Electronic Delivery Format

1. **Secure transmission**: All electronic documents transmitted for execution must be sent through a secure method, such as encrypted communication channel, a secure file-sharing platform, or equivalent.
2. **Delivery confirmation**: The electronic delivery system must provide confirmation of successful delivery to the intended recipients.
3. **Version control**: All transmitted documents should maintain version control to ensure the latest and most accurate version is being delivered and executed.

V. Alternative Continuity Process

Alternative processes may be used to provide secure, lawful, and efficient means of executing signatures remotely when technology authentication is not available. This applies to situations where the authorized signatories are unable to use the electronic signature solution due to technical issues, unavailability of necessary equipment, or other valid reasons, and require the manual completion of a remote signature process. Under the guidance and approval of the County Law Director, such processes are to ensure continuity in signing resolutions, ordinances, contracts, agreements, instruments, and other documents within Cuyahoga County, while adhering to legal standards and best practices refered to in the APPENDIX. Such a process should only be used in exceptional circumstances, under the strict oversight and approval of the County Law Director.

1. **Request for Alternative Continuity Process**: The requestor (such as the County Executive, or an authorized signing designee) must notify the County Law Director and the Department of Information Technology as soon as they become aware of the issue preventing the use of the standard electronic signature process.
2. **Assessment and Approval**: The County Law Director, in consultation with the Department of Information Technology, will assess the situation and determine whether an exception is warranted. If approved, the County Law Director will provide specific instructions for executing the signatures remotely and securely.
3. **Remote Signature Procedure**: Depending on the circumstances, the remote signature procedure may involve:
    a. Scanning and emailing the signed documents.
    b. Using a secure fax transmission.
    c. Sending photos of the signed documents via secure means.
    d. Other methods as approved by the County Law Director in consultation with the Department of Information Technology.
4. **Authentication:** The requestor must ensure the identity of the individual signing the document by either:
    a. A video conference where the signing is visibly seen.
    b. A phone call where the individual verbally confirms their identity and their intent to sign the document.
    c. Other methods as approved by the County Law Director in consultation with the Department of Information Technology.
5. **Delivery**: The signed documents must be delivered securely to the intended recipients. This may involve using encrypted email or other secure delivery methods, as directed by the County Law Director in consultation with the Department of Information Technology.

VI. Document Storage and Retention

1. **Secure storage**: All executed electronic documents must be stored securely in a repository with access limited to authorized individuals.
2. **Document encryption**: All stored documents must be encrypted to protect sensitive information and comply with data privacy regulations.
3. **Retention policies**: All executed documents will be stored in accordance with County Retention Policy and the Department of Information Technology retention policy.

VII. Training and Awareness

1. **Staff training**: The Department of Information Technology and the Department of Purchasing must make available training to all relevant staff members on the electronic delivery and execution processes, security protocols, and the use of the electronic signature solution.
2. **Awareness campaigns**: The Department of Information Technology must make available periodic awareness campaigns to reinforce the importance of security and compliance with these procedures in accordance with Section 302.03 of the Cuyahoga County Code.

VIII. Monitoring and Compliance

1. **System monitoring**: The Department of Information Technology must continuously monitor electronic delivery and execution systems for unauthorized access, potential vulnerabilities, and security incidents.
2. **Periodic audits**: The Department of Information Technology may conduct periodic audits to ensure compliance with these procedures and identify areas for improvement.
3. **Incident response**: In event of a security incident, the Department of Information Technology must respond in accordance with the established incident response procedures for events related to electronic delivery and execution.

IX. Amendments and Updates

The Department of Information Technology may periodically review and update these procedures as needed to maintain compliance with legal requirements, best practices, and evolving technology.

X. Approval and Implementation

The procedures for Electronic Delivery and Execution of Legislation are subject to the approval of the County Law Director and, without objection by the County Executive and County Council President in accodance with County Code Section 110.03(A), will go into effect within seven (7) days of submission and being posted online.

The procedures for Electronic Execution of Contracts, Agreements, Instruments, and Other Documents are subject to the approval of the County Law Director in accodance with County Code Section 110.03(B) and will go into effect as directed by the County Law Director.

XI. Change Log

Date Approved	Date Submitted	Summary	Updated By	Approved By
09/11/2023	09/11/2023	Version 1.0 – County Code 110.03(A)(B)	Jeremy Mio	Rick Manoloff, Law Director
09/11/2023	09/11/2023	Version 1.0 – County Code 110.03(B)	Jeremy Mio	Paul Porter, Purchasing Director

APPENDIX – Legal Standards and Best Practices

Relevant legal standards and best practices for implementing a secure and reliable electronic signature solution include the following:

Legal Standards:

a. **Electronic Signatures in Global and National Commerce Act (E-SIGN Act)**: This U.S. federal law provides a legal framework for the use of electronic signatures and records in interstate and foreign commerce. It ensures that electronic signatures and records have the same legal validity and enforceability as traditional paper documents and handwritten signatures.
b. **Uniform Electronic Transactions Act (UETA)**: This state-level model law, provides a legal framework for the use of electronic signatures and records in transactions. It establishes the validity and enforceability of electronic signatures, ensuring that they have the same legal effect as traditional paper documents and handwritten signatures.The State of Ohio UETA is specified within Chapter 1306 of the Ohio Revised Code.

Security Best Practices:

a. **Strong encryption**: Implement end-to-end encryption for both the electronic signature process and the storage of signed documents. This ensures that sensitive information is protected from unauthorized access and tampering. Encryption must meet the Acceptable Encryption County policy.
b. **User authentication and non-reputidation**: Use strong authentication methods, such as multi-factor authentication (MFA), to ensure that only authorized individuals can access the electronic signature solution and sign documents. User Authetication must meet the Account and Authentication County policy.
c. **Timestamps and audit trails**: Record and maintain detailed audit trails and timestamps for each step of the electronic signature process. This provides a comprehensive record of the signing process and helps ensure non-repudiation.
d. **Third-party certification**: Select an electronic signature solution that has been certified by a reputable third-party organization for compliance with relevant security standards, such as the International Organization for Standardization (ISO) or the National Institute of Standards and Technology (NIST).
e. **Data privacy and protection**: Ensure that the electronic signature solution complies with applicable data privacy regulations, such as the General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA). This may include providing appropriate notice and obtaining consent from users, as well as maintaining secure storage and handling of personal data.
f. **Backup and disaster recovery**: Implement robust backup and disaster recovery processes to ensure that electronic signature data can be recovered in the event of a system failure, data loss, or other incidents.
g. **Regular security assessments**: Conduct periodic security assessments, including vulnerability scanning and penetration testing, to identify and address potential security risks in the electronic signature solution.
h. **Policy and procedure documentation**: Develop and maintain clear policies and procedures for the use of electronic signatures, including user roles and responsibilities, training requirements, and incident response procedures.

By adhering to these legal standards and best practices, a secure and reliable electronic signature solution can be implemented, ensuring the validity and enforceability of electronic signatures in accordance with applicable laws and regulations.