

**UMATILLA-MORROW COUNTY HEAD START (UMCHS), INC.
ELECTRONIC SIGNATURES POLICY AND PROCEDURE**

1. PURPOSE. This policy establishes the criteria for the use and validity of electronic signatures associated with internal electronic transactions within UMCHS, Inc.. They are intended to ensure that, as agency programs implement this technology, they do so in a manner that is both consistent across the agency and compatible with the practices of other government agencies. A uniform approach encourages cost effectiveness and potential for future connectivity and integration of enterprise-wide electronic processing applications.

This Policy defines an Electronic Signature used by an employee, contractor, or grantee of UMCHS, Inc. as having specific qualities:

- (1) shall be unique to the person using it,
- (2) shall be capable of reliable verification and
- (3) shall be linked to a record in a manner so that if the record is changed the electronic signature is invalidated.

2. SCOPE AND APPLICABILITY. This policy applies to any electronic transaction originated by any employee, contractor, or grantee working for UMCHS, Inc. that involves providing approval, authorization, or certification, via the use of electronic signature, for actions or data.

This policy specifically applies to any such electronic transaction that:

- (1) Is being implemented as a replacement for (or complement to) a paper form or document originated by an employee, contractor, or grantee of UMCHS, Inc.
- (2) Involves the use of agency wide data processing, data storage and data communications facilities;
- (3) Replaces (or complements) documents or forms that require originator signature certification; or
- (4) Involves, or implies, procurements, financial commitments, obligations, certification of time and attendance, or disbursements.

An electronic signature solution should not be considered when a requirements analysis indicates there is no clearly defined cost or productivity advantage to be gained from the application. If the requirements analysis demonstrates a clear need for encrypted signatures, then the application will conform to standards cited in applicable Federal Information Processing Standards (FIPS) and Agency policies.

3. BACKGROUND.

General

- (1) Innovations in computer technology now allow the creation, processing and maintenance of documents in electronic form -- without requiring creation of corresponding paper media.
- (2) Automated information processing is rapidly becoming the preferred mode for management and transfer of information in business and government. Automation of administrative procedures has demonstrated that:
 - (a) Information can be processed more quickly;
 - (b) Costs of re-keying data are diminished;
 - (c) Data accuracy is increased.

(3) Many forms and documents used in UMCHS, Inc. activities require signatures of the responsible parties. The uses of electronic signatures may include, but are not limited to:

- (a) Certification of the transmission, receipt, and authorization of data;
- (b) Authorization or approval of an official action.
- (c) Certification and validation of the accuracy of agency databases.

(4) Procedures for the use of electronic signatures in creating and processing documents must provide adequate safeguards for the application, transmission, verification, and security of a signature and any accompanying data or information. If security profiles are modified, the system should be equipped with an audit trail capability to provide the User ID, time and date of the last person who made the modifications.

(5) Pursuant to Par. 4, AUTHORITIES, of this policy, as such information migrates into an electronic environment, it is essential to ensure that all official documents are developed, processed, and maintained consistent with applicable Federal and agency policies regarding electronic recordkeeping.

EXISTING TECHNOLOGY FOR ELECTRONIC SIGNATURES

The following technology areas provide effective electronic signature systems:

(1) Signature authentication allows users to verify the approval authority of a transmission. It is usually used in combination with other technologies to provide a complete electronic signature system. Signature authentication methods include:

- (a) Personal identification numbers (PINs)
- (b) Passwords
- (c) Message Authentication Coding (MAC)

(2) Message authentication provides the ability to confirm that the message received is exactly the same as the message that was sent. A major concern associated with electronic forms and signatures is an unauthorized user's ability to change an electronic form after it has been signed.

(a) Message authentication systems use varying procedures to calculate a message authentication code (MAC) based on the contents of the message. Some of these processes may involve cryptographic techniques. For example, message authentication systems may use private key encryption to calculate the MAC, requiring that both the sender and receiver know the key.

(b) If the message changes, the MAC code calculated on the receiver's side will be different from the attached MAC code calculated on the sender's side.

(c) Message authentication may provide two forms of security. It:

(1) Verifies the information has not been altered from the moment the MAC was generated to the time it was checked.

(2) May also assure the receiver of the sender's identity, e.g. through shared knowledge of the secret key used to calculate the MAC.

(3) Data encryption systems conceal message meaning by changing intelligible messages into unintelligible ones to everyone except the transmitter and receiver. Data encryption:

- (a) Can be used to safeguard signatures and signature authentication codes from disclosure during transmission and when data files containing signatures are stored.
- (b) Requires the use of keys to encrypt and decrypt data.
- (c) Can use public key, private key, or secret key encryption algorithms.

(4) Access control systems are designed to limit access to computer systems, including operating system files, and applications, including application programs and data files. Limiting access to systems and applications limits the population of users that can actually append a signature code to a message. Access control systems, at a minimum, should provide user identification, login control, access authorization, and auditing capabilities.

4. AUTHORITIES.

The Paperwork Reduction Act of 1980 (P.L. 96-511)

The Computer Matching and Privacy Act of 1987, 5-USC-522a (as amended)

Computer Security Act of 1987

FIPSPUB46-1 -- Data Encryption Standard; Jan. 22, 1988

FIPSPUB140A -- General Security Requirements for Equipment Using the Data Encryption Standard; April 14, 1982

5. POLICY.

UMCHS, Inc. is committed to support the implementation of integrated electronic processing applications which expedite the workload and reduce duplicate activities, consistent with applicable Federal and agency policies regarding electronic recordkeeping and security.

For all UMCHS, Inc. internal administrative applications involving the use of electronic approval, signature and distribution procedures, an electronic signature will be deemed as legally binding as a paper signature, provided each application is developed, implemented, and monitored in accordance with this policy.

When a determination has been made to fully automate a paper-based system that employs written signatures, all affected agency offices shall use electronic signatures.

Any application involving the use of data processing, storage and communications systems will be considered an agency wide application and will conform to the use of electronic signature solutions stated in this policy.

When an electronic message containing a signature is signed, transmitted, and received, the following requirements must be met:

(1) Signature Authentication:

- (a) The electronic signature must establish sender/user authenticity;
- (b) It must be possible to assure with a reasonable degree of certainty that the sender's signature has not been forged;
- (c) Sufficient audit trails must be provided to resolve disputes, with a reasonable degree of certainty, involving cases where an individual disavows sending a message.

(2) Message Authentication:

- (a) It must be possible to assure, with a reasonable degree of certainty, that a document and its signature have not been changed after it is signed.

Electronic information and forms processing applications involving the use of electronic signatures must incorporate signature and message authentication, as above, and may incorporate the following additional considerations:

- (1) The need for the signature on a document to be obscured from disclosure during transmission (i.e., data encryption);
- (2) The need for only a few individuals to have access to signing, processing, or viewing capabilities (i.e., access control).

Consistent with the goal of agency wide compatibility, only digital signature applications are addressed by this policy. Analog or facsimile signatures are not necessarily electronic, may be forged, and will not be considered valid for determining signature authenticity.

6. RESPONSIBILITIES.

The Information Systems Director, Fiscal Director, and Human Resources Director are responsible for:

- (1) Reviewing all currently automated systems within their respective areas to determine applicability to this policy and establishing procedures to ensure current and future systems comply with the requirements of this policy.
- (2) Identifying a specific technical approach for all required technology areas that cost-effectively addresses the risks of the application.
- (3) Determining the level of security required for any proposed application of electronic signature

The Information Systems Director is responsible for:

- (1) Providing training and awareness about the policy;
- (2) Providing guidance and assistance in implementing this policy;
- (3) Ensuring that information security and Privacy Act issues have been met;
- (5) Periodically reviewing electronic signature applications to ensure that electronic records are being maintained in accordance with applicable Federal and agency policies and procedures.
- (6) Re-evaluating/revalidating the policy within 5 years of approval;
- (7) Developing and maintaining policies and procedures for the acceptable use of specific commercially available electronic signature hardware components and software.

UMCHS, Inc. Management staff are responsible for:

- (1) Assuring compliance with this policy and its procedures on distributed systems operated by their staff members;

Owners of electronic signature applications are responsible for compliance with the provisions of this policy.

7. DEFINITIONS.

Access Control - A method of providing security designed to limit access to computer systems and applications. Types of access control include:

User Identification Codes
Login Control

Automated Information Processing - The electronic creation, processing, and exchange of information without the creation of corresponding paper media.

Data Decryption - The process of converting cipher text (an encrypted message) into readable form.

Data Encryption - A security method which conceals message meaning by changing intelligible messages to unintelligible ones. Encryption is the process in which plaintext messages are converted into apparently random nonsense, called cipher text, using an encryption algorithm and a data encryption "key".

Data Encryption Key - A bit string that controls a data encryption algorithm. The data encryption algorithm will produce a different output depending on the specific key used.

Electronic Record - Any information that is recorded in a form that only a computer can process and that satisfies the definition of a Federal record in 44 USC 3301 (see Records below).

Electronic Reporting - The computer-to-computer exchange of information in a standard format via either an electronic (e.g., dial-up telecommunications links, dedicated computer-to-computer links) or magnetic (e.g., diskettes, tapes) medium.

Electronic Signature - A data element, entered into a computer by an authorized person, that is used for noting the ownership, approval, acceptance, or certification of another object (e.g., a document or message). Electronic signatures provide the same validation and authentication capabilities as hand written signatures.

Encryption Key Management - The generation, distribution, entry, and destruction of encryption keys. While data encryption algorithms are publicly known, depending on the specific key used, a unique output will be produced. Therefore, it is the encryption key that provides the desired security. Two key management systems exist:

Form - For the purpose of this policy, any paper or electronic document with blanks for the insertion of data or information, circulated within UMCHS, Inc., that requires approval involving signature certification (e.g., travel authorization, travel voucher, procurement request/purchase order, etc.).

Login Control - Specifies the conditions users and programs must meet for gaining access to a system. For example, a user usually requires a valid user ID and password before access to a system is provided. Additional methods used to control login include:

Type of computer login (e.g., local, dial-up, remote, network, batch)

Message Authentication - A method of detecting changes to a message after it has been signed electronically. After signing a message, the sender calculates a Message Authentication Code (MAC) based on the contents of the message. This code is appended to the message and transmitted. The message recipient performs the same calculations on the received message. If the calculated MAC and the received MAC are the same, the message was not altered after the message was signed.

Message Authentication Code (MAC) - The code used by message authentication systems to validate transmitted messages. This code is calculated by performing a series of mathematical calculations on a signed message.

Private Key - A cryptographic key used with a public key cryptographic algorithm, uniquely associated with an entity, and not made public.

Public Key - A cryptographic key used with a public key cryptographic algorithm, uniquely associated with an entity, and possibly made public.

Records - In records management, this term refers to recorded information of continuing administrative, fiscal, legal, historical or informational value, including published materials, papers, maps, photographs, microfilm, audiovisual, machine-readable materials (tapes/disks) or other documentary material, regardless of physical form or characteristics, made or received by the agency that evidences organizations, made or received by the agency that evidences organization, functions, policies, decisions, procedures, operations or other activities of UMCHS, Inc..

Risk Analysis - The process of methodically and comprehensively examining a system to identify the areas that pose a threat of failure to the system.

Secret Key - A cryptographic key used with a secret key cryptographic algorithm, uniquely associated with one or more entities, and not made public.

Signature Authentication - A code, used to identify the sender, appended to a message before transmission. This code is validated by the message recipient. A variety of user authentication techniques exist, including:

Personal identification numbers (PINs) – combination of alpha-numeric digits that protect and secure information and access control