600 NE Grand Ave.
Portland, OR 97232-2736
www.oregonmetro.gov

Metro | *Policies and procedures*

Subject Electronic Signature (E-Signature) Policy and Procedures

Section Information Services (IS)

Subsection Records and Information Management (RIM) program

Approved by Martha Bennett, Chief Operating Officer

POLICY

This policy provides guidelines for the use of electronic signatures (e-signatures) in conducting Metro business operations. This policy will ensure that Metro complies with applicable laws for paperless processing, along with established policies and procedures related to records and information management.

Applicable to

Applies to all employees, including Metro officials, temporary and seasonal employees, interns, volunteers, contractors, and consultants.

Definitions

Authentication:

1. Process of verifying that a record is what it purports to be.
2. To establish as genuine and to verify the identity of the person providing an electronic signature.

Authenticity: Sum of the qualities of a record that establish the origin, reliability, trustworthiness, and correctness of its content.

Certificate: An electronic document used to identify an individual, server, a company, or some other entity and to associate that identity with a public key. A certificate provides generally recognized proof of a person's identity. (See Public Key Infrastructure)

Chain of Custody: Auditable and court admissible documentation of the possession, condition, location, transfer, access to and any analysis performed on an item from acquisition through eventual final disposition.

Context: The organizational, functional, and operational circumstances in which documents are created and/or received and used. Also, the placement of records with a larger records classification system providing cross-references to other related records.

Digital Signature: A type of electronic signature that transforms 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 (ORS 192.835(4)).

Electronic Record or e-record: A record created, generated, sent, communicated, received, or stored by electronic means. "Electronic records" does not include or refer to photocopies, digital imaging systems, or analog or digital audio and videotapes.

Electronic Signature or e-Signature:

1. An electronic sound, symbol or process attached to or logically associated with a record and executed or adopted by a person with the intent to authenticate the record.
2. Refers to a number of technologies that allow a person (or machine) to electronically "mark" a document. In doing so, the document is provided some level of authentication by "locking down" the document's content at the time it is signed, retaining certain characteristics for evidentiary purposes.

Electronic Transaction or e-Transaction: An action or set of actions that is conducted or performed, in whole or in part, by electronic means and/or via electronic records.

Integrity: Refers to a record being complete and unaltered overtime; implies a reasonable and suitable guarantee of the record's authenticity and reliability for its life cycle.

Life cycle: The distinct phases of a record's existence, including creation, distribution, use, maintenance, and disposition of a record.

Public Key Infrastructure (PKI): A system of people, processes, and technology for issuing and managing digital certificates that can be used for online identification, digital signing, and other information security-related functions. PKI systems use two different keys. One is kept secret (the private key) and the other key is made publically available (the public key). The two keys are generated simultaneously and collectively; they are known as the "key pair." Once a message has been signed using one of the two keys, it can only be verified by the other key. The resulting digital signature is a cryptographic checksum computed as a function of the message and the signer's private key.

Recordkeeping System: A specialized version of an information system that captures, maintains, and provides access to records as evidence over time and allows for disposition according to records retention schedules.

Reliability: The characteristics of a record that demonstrate that it can be trusted as a full and accurate representation of the transactions, activities, or facts to which it attests [ISO 15489].

Repudiation:

1. Denial by the purported author of a message that the message was created by him or her.
2. Claim by an author of a message that the content of the message was altered after the message was sent.

Retention Schedule: A comprehensive list of records series that indicates for each the record series the length of time it is to be maintained and its disposition.

Security Procedure: A procedure that is employed to verify that an electronic signature, record or performance is that of a specific person, to determine that the person is authorized to sign the document and to detect changes or errors in the information in an electronic record. This includes a procedure that requires the use of algorithms or other codes, indentifying words or numbers or encryption, callback or other acknowledgment procedures.

Structure: The physical land logical format of a record and the relationships between the data elements.

Additional terms relating to e-signatures used throughout this document are defined in Metro's *Glossary of Records and Information Management Terms,* which is maintained on the RIM program website.

Authority

- Public Law No. 106-229 - Electronic Signatures in Global and National Commerce Act (ESIGN)
- ORS 84 - Oregon Uniform Electronic Transactions Act (UETA)
- OAR 125-600-0005 – Guidelines for Use of Electronic Signatures by State Agencies
- Metro Records and Information Management (RIM) Policy

Federal and state legislation give legal force and effect to electronic or digital signatures, granting e-signatures and e-records equal stature with their physical counterparts. With few exceptions, e-signatures and e-records cannot be denied legal effect solely because they are electronic.

ESIGN gives electronic contracts the same weight as those executed on paper. Although the act enables documents to be signed electronically, the option to do so lies solely with the consumer. The onus is on the organization to determine how it plans to meet the requirements for capturing signing intent and authenticating data and signers.

UETA provides a legal framework for electronic transactions. It gives electronic signatures and records the same validity and enforceability as manual signatures and paper-based transactions. UETA created legal recognition for most electronic transactions and parallels the legal recognition for paper transactions conducted in Oregon.

These laws are purposefully technology-neutral, meaning they do not prescribe specific technologies, except to indicate that the technologies must be mutually acceptable to the transacting parties. This is done to prevent legislative obsolescence in the face of new technologies, but also because more than one technology is available and a comprehensive solution could make use of combinations of them.

The Chief Operating Officer delegates to the Records Officer the authority to update this policy and procedures as circumstances dictate.

Guidelines

1. This policy provides a framework for business units to use when considering implementation of e-signature. Eliminating paper-based tasks (where appropriate) and implementing e-signature solutions can improve information security and sharing, allow quicker access to documents, and reduce costs and environmental impact. Streamlining processes requiring traditional “wet” signatures and replacing them with e-signatures can also reduce transaction processing time.

2. This policy is not a mandate to replace handwritten signatures, but rather a policy to integrate e-signatures into Metro’s business processes.

3. Metro staff may use and maintain records and signatures in electronic formats during the normal course of business activities. Electronic records and electronic signatures shall be regarded by Metro as equivalent to paper records and traditional signatures.

4. E-signatures may be implemented using various methodologies depending on the risks associated with the transaction. Since a valid signature can be as simple as a scanned image of a signature or as complex as public key infrastructure (PKI) methods, business units must define relevant business objectives and understand the risks, such as cost and the potential for unauthorized use.

5. The quality and security of the e-signature method should be commensurate with the risk and needed assurance of the authenticity of the signer. Authentication features ensure that the user who employs an e-signature is in fact who they say they are and is authorized to “sign”.

6. Because the use of e-signature carries an element of risk, especially that which relates to acceptable use, it is necessary to have robust provisions in place to protect access to and regulate the use of e-signatures. In addition, before selecting and deploying an e-signature solution, it is important to conduct a legal review of a proposed application or process to ensure legal sufficiency, reliability, and compliance with existing laws and regulations. An Agency-approved e-signature process that adheres to practical security procedures and balances risk and cost, while assuring data integrity and non-repudiation, will satisfy legal sufficiency and reliability concerns.

7. By itself, no e-signature technology is sufficient to meet all legal needs. The evidentiary value of signed records ultimately relies on the Agency's ability to produce legally admissible documentation of its recordkeeping system. Hence, electronic records and e-signatures need to be created and maintained in reliable and secure systems that ensure their authenticity and acceptability as evidence in a court of law.

8. Business units must also consider records management requirements when planning, implementing and maintaining e-signature processes and technologies. Based on retention requirements (as per Metro's Records Retention Schedule) and risks associated with technological obsolescence, the trustworthiness of the electronically signed record must be ensured for its life cycle.

9. It is not the intent of this policy to eliminate all risk, but rather to provide a process for undertaking an appropriate analysis prior to approving the use of e-signatures for specific Agency transactions.

Responsibilities

All Metro employees are expected to adhere to this policy and set of procedures as part of their records management responsibilities under Metro Records and Information Management (RIM) Policy. RIM staff will advise and answer questions regarding this and any other RIM policies and procedures.

Any individual or party that makes inappropriate or illegal use of e-signatures and/or records would contradict the requirements of this policy and could lead to sanctions up to and including disciplinary action, dismissal, and criminal prosecution as specified in Agency policies, and State laws, whether or not they are referenced in this policy.

References

- *Metro's Glossary of Records and Information Management Terms*
- *Metro's Records Retention Schedule*
- *Metro Records and Information Management (RIM) Policy*

Additional Information

For further information regarding this or any other records and information management (RIM) policy, contact Metro's records officer or refer to the Records and Information Management (RIM) program website.

PROCEDURES

These procedures provide general guidance to Metro workgroups planning and implementing electronic signature (e-signature) as a component of business operations.

Terms used throughout this set of procedures are used as defined in Metro's *Glossary of Records and Information Management Terms*, which is maintained on the RIM program website.

Evaluation

When undertaking an e-signature initiative, staff should evaluate and select an e-signature methodology based on their business needs. In brief, those methodologies include:

- an approval conveyed through email signature
- a scanned image of an original signature
- an Adobe-generated e-signature
- a "click through" option (used on many web sites and designed to move an individual from "A" to "C" only through "B," with "B" serving as the equivalent of a signature
- a digital signature (enabled through the use of specific PKI technology that is either managed in-house or hosted through a third party provider)

There are two general categories of e-signature solutions:

- a dedicated, on premises solution that is deployed behind an organization's firewall
- a multi-tenant cloud service

Which methodology and solution is the best fit will depend on:

- the complexity of the business process requiring automation
- the level of integration with an organization's front and back-end systems
- availability of IT and budgetary resources
- implementation timeframe requirements

The following guidelines identify key elements of the evaluation process:

1. ***Goals and Objectives***: The goals and objectives of the e-signature initiative should be clearly defined.

2. ***Business Requirements***: A description of the business process impacted by the implementation of e-signature should be completed, including current workflow and recordkeeping practices and anticipated changes to those practices.

3. ***Risk Assessment***: An evaluation of risk will be performed by the business unit to determine risks associated with using an e-signature and to determine the quality and security of the e-signature method required. An evaluation will be made using the *E-Authentication Guidance for Federal Agencies, OMB 04-04*. [See: Attachment No. 1]

4. ***Specifications***: Business units need to address security specifications for recording, documenting, managing and/or auditing the e-signature as required for non-repudiation and other legal requirements. Security features to look for in an e-signature solution include:
   - **User Authentication**: the process of identifying an individual and ensuring that the person is who he or she claims to be.
   - **Data Authentication**: the process of verifying the information contained in a signed document to ensure that it has not changed since it was signed.
   - **Process Control**: Electronic transactions can be controlled by workflow rules to reduce the risk of non-compliance and errors.
   - **Process Evidence**: to prove exactly what took place at every state of the document review and signing process.

Additional requirements to consider when defining the right e-signature solution are:

- **Ease of Use**: the solution should be easy for the end user to utilize.
- **Process Flexibility**: the solution should fit the existing business process as closely as possible to minimize process re-engineering.
- **Scalability**: the solution should be capable of supporting a variety of business processes and lines of business across the enterprise.
- **Evidence**: the solution should ensure that e-evidence can be easily produced and presented in the event of a legal dispute.

Guidelines from the National Institute of Standards and Technology (NIST) can be useful in assessing security specifications for e-signature solutions.

5. ***Records Management Requirements****:* E-signatures become an integral part of a record. Therefore, measures need to be taken to ensure the trustworthiness of the electronically-signed record for its life cycle. When planning an e-signature implementation, certain characteristics need to be considered to ensure the e-signature method can meet internal business and legal needs, and external regulations or requirements. The following characteristics of trustworthy records have been identified by the National Archives and Records Administration (NARA):

    - **Reliability**: A reliable record attests to the trustworthiness of the record's content - that it is a "full and accurate representation of the transactions, activities, or facts to which it attests and can be depended upon in the course of subsequent transactions or activities."
    - **Authenticity**: An authentic record is one that is proven to be what it claims to be and to have been created or sent by the person who claims to have created and sent it. In demonstrating the authenticity of records, business units should "*implement and document policies and procedures which control the creation, transmission, receipt, and maintenance of records to ensure that records creators are authorized and identified and that records are protected against unauthorized addition, deletion, and alternation*."
    - **Integrity**: The integrity of a record refers to it being complete and unaltered. The authenticity and reliability of an electronically signed record can be upheld by tracking the chain of custody and any changes that may occur (authorized or unauthorized), and preserving the physical format and relationships between the data elements comprising the record over its life cycle.
    - **Usability**: For a record to be usable, it needs to be easily located, retrieved and interpreted. The context of the record – how it is connected to a business activity or a business transaction that produced it - should be readily identifiable and understood. "*The contextual linkages of records should carry the information needed for an understanding of the transaction that created and used them*."

Approval Process

The business unit will seek approval to implement an e-signature using the *Electronic Signature (E-Signature) Proposal Form*. [See: Attachment No. 2] It is the business unit's responsibility to ensure that the proposed e-signature method and solution meet the requirements of this policy. In determining whether to approve an e-signature method and solution, consideration will be given to the systems and procedures associated with using the e-signature and whether its use is at least as reliable as the existing method being used.

Upon completion, the *E-Signature Proposal Form* needs to be submitted to the E-Signature Review Team - a cross-functional group comprised of Information Services and Office of Metro Attorney staff. The team will review the e-signature proposal and provide comments and recommendations for implementation.

Implementation
When the evaluation and approval process for the e-signature method and solution are completed, business units need to work with Information Services staff to plan the e-signature implementation process. In general, the implementation process will differ for each type of transaction and for each business unit, as it is dependent on many factors such as technical environment, appropriate assurance level, and the nature of the transaction. In addition, provisions need to be made to test the application after implementation to validate that the authentication system has operationally achieved the required assurance level.

Once a process for an Agency e-signature transaction is approved and automated, it is immediately subject to the provisions of this policy.

Training
User adoption and adherence to standards and best practices are critical success factors in implementing new business processes and deploying new technologies. Business units undertaking e-signature initiatives need to define a change management strategy that includes an assessment of staff training requirements. Based upon the degree of change and complexity of the e-signature methodology, business units need to address the following elements when designing a training plan:

- level(s) of training required
- method of delivering training (e.g., insourcing vs. outsourcing; classroom vs. on-line)
- curriculum requirements
- budget impacts
- training schedule
- ongoing training requirements (based upon system upgrades and staff turnover)

Maintenance and Review Requirements
Upon implementation of an e-signature technology, the following should be addressed on an ongoing basis:

1. ***Recordkeeping***: A formal record of the risk assessment evaluation, e-signature method selection, and justification will be maintained by the business unit and Information Services.
2. ***Security****:* The business unit will work with Information Services staff to ensure that appropriate controls and monitoring of the e-signature or digital signature software/hardware are in place.
3. ***Review***: The business unit will periodically conduct a review of each e-signature implementation. The review will include:

    - an evaluation of the e-signature use to determine if any applicable legal, business, or data requirements have changed
    - a determination regarding the continued appropriateness of the risk assessment and e-signature implementation method

    A record of this review will be documented and filed as part of the official record for this e-signature implementation maintained by the business unit. If, as a result of the periodic review, the risk level changes, a new risk assessment must be completed, including review and approval.

Resources

- *E-Authentication Guidance for Federal Agencies, OMB 04-04, December 16, 2003*
- *Electronic Authentication Guidelines, National Institute of Standards and Technology (NIST), Special Publication 800-63, ver. 1.02.2, April 2006*
- *PKI Assessment Guidelines: Guidelines to Help Assess and Facilitate Interoperable Trustworthy Public Key Infrastructures, American Bar Association, 2003*
- *Records Management Guidance for Agencies Implementing Electronic Signature Technologies, National Archives and Records Administration (NARA), October 18, 2000*

- *Records Management Guidance for PKI Digital Signature Authenticated and Secured Transaction Records, National Archives and Records Administration (NARA), March 11, 2005*
- *Oregon State University Administrative Policies & Procedures, Fiscal Operations(FIS) Manual: e-Signature, June 30, 2008*

Attachments

- *E-Signature Authentication Assurance Levels*
- *Electronic Signature (E-Signature) Proposal Form*

E-Signature Authentication Assurance Levels

Excerpt from *E-Authentication Guidance for Federal Agencies, OMB 04-04;* memorandum dated December 16, 2003.

Description of Assurance Levels

This guidance describes four identity authentication assurance levels for e-government transactions. Each assurance level describes the agency's degree of certainty that the user has presented an identifier (a credential in this context) that refers to his or her identity. In this context, assurance is defined as 1) the degree of confidence in the *vetting process* used to establish the identity of the individual to whom the credential was issued, and 2) the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued. The four assurance levels are:

- Level 1: Little or no confidence in the asserted identity's validity.
- Level 2: Some confidence in the asserted identity's validity.
- Level 3: High confidence in the asserted identity's validity.
- Level 4: Very high confidence in the asserted identity's validity.

Potential Impact Categories: To determine the appropriate level of assurance in the user's asserted identity, agencies must assess the potential risks, and identify measures to minimize their impact. Authentication errors with potentially worse consequences require higher levels of assurance. Business process, policy, and technology may help reduce risk. The risk from an authentication error is a function of two factors:

1. potential harm or impact, and
2. the *likelihood* of such harm or impact.

Categories of harm and impact include:

- Inconvenience, distress, or damage to standing or reputation
- Financial loss or agency liability
- Harm to agency programs or public interests
- Unauthorized release of sensitive information
- Personal safety
- Civil or criminal violations.

Required assurance levels for electronic transactions are determined by assessing the potential impact of each of the above categories using the potential impact values described in Federal Information Processing Standard (FIPS) 199, "Standards for Security Categorization of Federal Information and Information Systems." The three potential impact values are:

- Low impact
- Moderate impact
- High impact.

The next section defines the potential impacts for each category. Note: If authentication errors cause no measurable consequences for a category, there is "no" impact. Determining Potential Impact of Authentication Errors:

Potential impact of ***inconvenience, distress, or damage to standing or reputation***:

- **Low** - at worst, limited, short-term inconvenience, distress or embarrassment to any party.
- **Moderate** - at worst, serious short term or limited long-term inconvenience, distress or damage to the standing or reputation of any party.
- **High** - severe or serious long-term inconvenience, distress or damage to the standing or reputation of any party (ordinarily reserved for situations with particularly severe effects or which affect many individuals).

Potential impact of ***financial*** *loss*:

- **Low** - at worst, an insignificant or inconsequential unrecoverable financial loss to any party, or at worst, an insignificant or **inconsequential** agency liability.
- **Moderate** - at worst, a serious unrecoverable financial loss to any party, or a serious agency liability.
- **High** - severe or catastrophic unrecoverable financial loss to any party; or severe or catastrophic agency liability.

Potential impact of ***harm to agency programs or public interests***:

- **Low** - at worst, a limited adverse effect on organizational operations or assets, or public interests. Examples of limited adverse effects are: (i) mission capability degradation to the extent and duration that the organization is able to perform its primary functions with noticeably reduced effectiveness, or (ii) minor damage to organizational assets or public interests.
- **Moderate** - at worst, a serious adverse effect on organizational operations or assets, or public interests. Examples of serious adverse effects are: (i) significant mission capability degradation to the extent and duration that the organization is able to perform its primary functions with significantly reduced effectiveness; or (ii) significant damage to organizational assets or public interests.
- **High** - a severe or catastrophic adverse effect on organizational operations or assets, or public interests. Examples of severe or catastrophic effects are: (i) severe mission capability degradation or loss of to the extent and duration that the organization is unable to perform one or more of its primary functions; or (ii) major damage to organizational assets or public interests.

Potential impact of ***unauthorized release of sensitive information***:

- **Low** - at worst, a limited release of personal, U.S. government sensitive, or commercially sensitive information to unauthorized parties resulting in a loss of confidentiality with a low impact as defined in FIPS PUB 199.
- **Moderate** - at worst, a release of personal, U.S. government sensitive, or commercially sensitive information to unauthorized parties resulting in loss of confidentiality with a moderate impact as defined in FIPS PUB 199.
- **High** - a release of personal, U.S. government sensitive, or commercially sensitive information to unauthorized parties resulting in loss of confidentiality with a high impact as defined in FIPS PUB 199.

Potential impact to ***personal safety***:

- **Low** - at worst, minor injury not requiring medical treatment.
- **Moderate** - at worst, moderate risk of minor injury or limited risk of injury requiring medical treatment.
- **High** - a risk of serious injury or death.

The potential impact of ***civil or criminal violations*** is:

- **Low** - at worst, a risk of civil or criminal violations of a nature that would not ordinarily be subject to enforcement efforts.
- **Moderate** - at worst, a risk of civil or criminal violations that may be subject to enforcement efforts.
- **High** - a risk of civil or criminal violations that are of special importance to enforcement programs.

Determining Assurance Level

Compare the impact profile from the risk assessment to the impact profiles associated with each assurance level, as shown in Table 1 below. To determine the required assurance level, find the lowest level whose impact profile meets or exceeds the potential impact for every category analyzed in the risk assessment (as noted in step 2 below).

Table 1 – Maximum Potential Impacts for Each Assurance Level

	Assurance Level Impact Profiles			
Potential Impact Categories for Authentication Errors	**1**	**2**	**3**	**4**
Inconvenience, distress or damage to standing or reputation	Low	Mod	Mod	High
Financial loss or agency liability	Low	Mod	Mod	High
Harm to agency programs or public interests	N/A	Low	Mod	High
Unauthorized release of sensitive information	N/A	Low	Mod	High
Personal Safety	N/A	N/A	Low	Mod High
Civil or criminal violations	N/A	Low	Mod	High

Assurance Levels and Risk Profiles: Descriptions and Examples

Level 1 - Little or no confidence exists in the asserted identity. For example, Level 1 credentials allow people to bookmark items on a web page for future reference.

Examples:

- In some instances, the submission of forms by individuals in an electronic transaction will be a Level 1 transaction: (i) when all information is flowing to the Federal organization from the individual, (ii) there is no release of information in return, and (iii) the criteria for higher assurance levels are not triggered. For example, if an individual applies to a Federal agency for an annual park visitor's permit (and the financial aspects of the transaction are handled by a separate contractor and thus analyzed as a separate transaction, the transaction with the Federal agency would otherwise present minimal risks and could be treated as Level 1.
- A user presents a self-registered user ID or password to the U.S. Department of Education web page, which allows the user to create a customized "My.ED.gov" page. A third party gaining unauthorized access to the ID or password might infer personal or business information about the individual based upon the customization, but absent a high degree of customization however, these risks are probably very minimal.
- A user participates in an online discussion on the whitehouse.gov website, which does not request identifying information beyond name and location. Assuming the forum does not address sensitive or private information, there are no obvious inherent risks.

Level 2 - On balance, confidence exists that the asserted identity is accurate. Level 2 credentials are appropriate for a wide range of business with the public where agencies require an initial identity assertion (the details of which are verified independently prior to any Federal action).

Examples:

- A user subscribes to the Gov Online Learning Center (www.golearn.gov). The site's training service must authenticate the person's identity to present the appropriate course material, assign grades, or demonstrate that the user has satisfied compensation-or promotion-related training requirements. The only risk associated with this transaction is a third party gaining access to grading information, thereby harming the student's privacy or reputation. If the agency determines that such harm is minor, the transaction is Level 2.
- A beneficiary changes her address of record through the Social Security web site. The site needs authentication to ensure that the entitled person's address is changed. This transaction involves a low risk of inconvenience. Since official notices regarding payment amounts, account status, and records of changes are sent to the beneficiary's address of record, it entails moderate risk of

unauthorized release of personally sensitive data. The agency determines that the risk of unauthorized release merits Assurance Level 2 authentication.

- An agency program client updates bank account, program eligibility, or payment information. Loss or delay would significantly impact him or her. Errors of this sort might delay payment to the user, but would not normally result in permanent loss. The potential individual financial impact to the agency is low, but the possible aggregate is moderate.
- An agency employee has access to potentially sensitive personal client information. She authenticates individually to the system at Level 2, but technical controls (such as a virtual private network) limit system access to the system to the agency premises. Access to the premises is controlled, and the system logs her access instances. In a less constrained environment, her access to personal sensitive information would create moderate potential impact for unauthorized release, but the system's security measures reduce the overall risk to low.

Level 3 - Level 3 is appropriate for transactions needing high confidence in the asserted identity's accuracy. People may use Level 3 credentials to access restricted web services without the need for additional identity assertion controls.

Examples:

- A patent attorney electronically submits confidential patent information to the US Patent and Trademark Office. Improper disclosure would give competitors a competitive advantage.
- A supplier maintains an account with a General Services Administration Contracting Officer for a large government procurement. The potential financial loss is significant, but not severe or catastrophic, so Level 4 is not appropriate.
- A First Responder accesses a disaster management reporting website to report an incident, share operational information, and coordinate response activities.
- An agency employee or contractor uses a remote system giving him access to potentially sensitive personal client information. He works in a restricted-access Federal office building. This limits physical access to his computer, but system transactions occur over the Internet. The sensitive personal information available to him creates a moderate potential impact for unauthorized release.

Level 4 - Level 4 is appropriate for transactions needing very high confidence in the asserted identity's accuracy. Users may present Level 4 credentials to assert identity and gain access to highly restricted web resources, without the need for further identity assertion controls.

Examples:

- A law enforcement official accesses a law enforcement database containing criminal records. Unauthorized access could raise privacy issues and/or compromise investigations.
- A Department of Veterans Affairs pharmacist dispenses a controlled drug. She would need full assurance that a qualified doctor prescribed it. She is criminally liable for any failure to validate the prescription and dispense the correct drug in the prescribed amount.
- An agency investigator uses a remote system giving her access to potentially sensitive personal client information. Using her laptop at client worksites, personal residences, and businesses, she accesses information over the Internet via various connections. The sensitive personal information she can access creates only a moderate potential impact for unauthorized release, but her laptop's vulnerability and her non-secure Internet access raise the overall risk.

Electronic Signature (E-Signature) Proposal Form

This form is designed to assist with the scoping, planning, and implementation of electronic signature initiatives at Metro. All applicable sections of this form are to be completed by the responsible unit in cooperation with Information Services (IS) and Office of Metro Attorney (OMA) staff (if required). Upon completion, the form is to be maintained and updated as necessary by the responsible unit, and a reference copy will be maintained on file by IS.

> Terms related to e-signature used throughout this Worksheet are used as defined in Metro's *Glossary of Records and Information Management Terms*, which is maintained on the RIM program intramet web

Section I. GENERAL INFORMATION

Requesting Unit: _____

Primary Unit Contact: _____

Electronic Signature Initiative Description: _____

1. What is the goal/objective of this e-signature initiative?
   (e.g., *eliminating paper-based tasks to reduce costs and increase productivity/efficiency, streamlining internal and external workflow by reducing transaction processing time, more efficient recordkeeping, improved accessibility by staff and/or the public)*

2. Provide a detailed description of the business process that will be impacted by this initiative, and who will have to use and rely on e-signature (*e.g., internal staff, external customers or both*).

3. Describe electronic authentication method for this transaction and how it meets the risks identified in the e-Signature Authentication Assurance Levels.
   [*Note: See Attachment No. 1: E-Signature Authentication Assurance Levels*]

4. Describe any data integrity and audit requirements for this transaction, and how they will be met.

5. Describe any security or access control requirements, and how they will be met.

6. Describe the records management requirements for this transaction, including measures that will be taken to ensure the reliability, authenticity, integrity and usability of e-signed records for their life cycle.
   [*Note: Please include how long the e-signature affixed to the electronic records will need to be preserved*]

Section II. Assessment of Electronic Signature Solution

Based upon the nature of the e-signature initiative (as described), provide an assessment of the e-signature methodology that best meets the needs of the transaction and how the e-signature technology will fit into Metro's overall technology architecture? (e.g., *scanned signature, Adobe e-signature, "click through", digital signature)*.

Section III. Training and Evaluation

Based upon the nature of the e-signature proposal, please describe the plan for staff training and monitoring of the e-signature initiative.

Section IV. Review /Recommendations for Implementation

As required, the E-signature Review team has evaluated this e-signature proposal and has made the following recommendations:

☐ Approved	☐ Approved with conditions (as described above)	☐ Disapproved

Signature & Date: _____ _____

(E-Signature Review team representative) Date