Informal Solicitation No. 1193001

MONTGOMERY COUNTY
DEPARTMENT
OF
ENVIRONMENTAL PROTECTION

PDF Remediation for ADA Accessibility Compliance

Issued: January 22, 2026

INFORMAL SOLICITATION #1193001
FOR
PDF REMEDIATION FOR ADA ACCESSIBILITY COMPLIANCE

ISSUE DATE: January 22, 2026, 11:00AM
SUBMISSION DEADLINE: January 30, 2026, 3:30PM

The Montgomery County Department of Environmental Protection is soliciting proposals for PDF REMEDIATION FOR ACCESSIBILITY COMPLIANCE. Proposals must be submitted no later than the date and time listed above. If an offeror is interested in submitting a proposal but cannot make the submission deadline, the offeror must call/email the Department of Environmental Protection at DEP.Procurements@montgomerycountymd.gov to see if an extension may be granted.

The following pages contain the terms, conditions, and scope of services for this Informal Solicitation.

Submit proposals to DEP.Procurements@montgomerycountymd.gov.

Should you have any questions regarding the information, or the scope of services contained in this solicitation, contact DEP.Procurements@montgomerycountymd.gov.

Bidding/Offer Submission Instructions:

Bids/Offers will only be accepted in an electronic format either as an Adobe® PDF (preferred) document or as a Microsoft® Word document. Offers MUST be submitted by e-mail to DEP.Procurements@montgomerycountymd.gov and the files must be received no later than the proposal due date and time shown above. The County's e-mail timestamp will be the determination of timely submission or not.

- The maximum file size that can be submitted is 30 Megabytes, therefore, Offerors must ensure the bid/offer file is compressed to reduce the file size below that threshold. This includes, but is not limited to, compressing all images and deleting any cropped areas, flattening layered images, and optimizing image quality to reduce their size, PDF files should be compressed before sending.
- Bidders/Offerors must ensure the file is not too large for their mail server to transmit as well.
- The e-mail submission of a link to download a larger file (Dropbox, SharePoint, OneDrive, etc.) will not be accepted.
- It is the Bidders/Offerors responsibility to ensure the transmission of the bid/offer has been successful. When a bid/offer is received, a reply will be sent confirming receipt of the bid/offer within one business day. Use the contact information above, or call 240-777-7787, to contact the DEP Contracts Team if you do not receive a confirmation within one business day.
- If the Bidder/Offeror uses a non-Adobe® PDF-making product, it is the Bidders/Offerors responsibility to ensure the file is readable by Adobe® Reader, a free program provided by Adobe. If the Bid/Offer documents are not readable or are incomplete (e.g., form field contents do not display in the Adobe product) the bid/offer will be deemed non-responsive and will be rejected. It is recommended that users print the document or file from the non-Adobe product to the PDF Printer to flatten the file and remove any form fields.

TABLE OF CONTENTS

Montgomery County, Maryland
ACKNOWLEDGMENT PAGE

ACKNOWLEDGMENT

The offeror must include a signed acknowledgment that all the provisions, terms and conditions of this solicitation are agreeable to the offeror and may, at the County's option, be made applicable in any contract issued as a result of this solicitation. Offers that do not include such an acknowledgment may be rejected. Executing and returning (with the offer) the acknowledgment shown below will satisfy this requirement.

The undersigned agrees that all the provisions, terms and conditions of this solicitation may, at the County's option, be made applicable in any contract issued as a result of this solicitation.

Business Firm's Legal Name (printed): ______________________________

Printed Name, Title and E-Mail of Person Authorized to Sign Proposal: ______________________________

Signature: Date:

NAME AND SIGNATURE REQUIREMENTS FOR PROPOSALS AND CONTRACTS

The correct and full legal business name of the offeror must be used in proposals received and on all contracts issued as a result of this solicitation. A trade name (i.e., a shortened or different name under which the firm does business) must not be used when the legal name is different. Corporations must have names that comply with State law, which requires a suffix indicating the corporate status of the business (e.g., Inc., Incorporated, etc.). Trade names may be indicated by individuals or corporations with the individual or corporate name followed by “t/a” (trading as) or “d/b/a’ (doing business as), respectively. The offeror’s signature on the proposal, contract, amendment(s) or related correspondence, must conform to the following:

All signatures must be made by an authorized officer, partner, manager, member, or employee. The signing of this offer or a contract is a representation by the person signing that the person signing is authorized to do so on behalf of the offeror or contractor.

ACKNOWLEDGMENT OF SOLICITATION AMENDMENTS

The Offeror acknowledges receipt of the following amendment(s) to the solicitation:

Amendment Number	Date

SECTION A. INSTRUCTIONS, CONDITIONS AND NOTICES

1. INTENT

The Intent of this Informal Solicitation is to solicit proposals for the procurement of PDF Remediation For Accessibility Compliance for Montgomery County, Maryland, as per the Terms, Conditions, Specifications, and/or Scope of Work, and Quotation Sheet contained herein.

2. PROPOSAL SUBMISSION

Proposals must be submitted no later than **3:30 pm EST**, **January 30, 2026,** to: DEP.Procurements@montgomerycountymd.gov.

Proposals submitted after 3:30 pm EST, **January 30, 2026, will not be considered.**

There will not be a pre-submission conference.

Questions must be received no later than 24 hours before the solicitation closes, inclusive of any extensions issued by Amendment.

3. VERBAL EXPLANATIONS

Verbal explanations or instructions given by a Montgomery County employee to an offeror in regard to this Informal Solicitation will not be binding on the County. Any information given to an offeror, in response to a request, will be furnished to all offerors as Solicitation Amendment to this Informal Solicitation, if such information is deemed necessary for the preparation of proposals, or if the lack of such information would be detrimental to the uninformed offerors. Only such amendments issued by the Contracting Officer will be considered as being binding on the County.

4. AWARD OR REJECTION OF OFFERS

The County reserves the right to accept or reject any or all offers, or portions thereof, to waive minor irregularities and to award the Contract in the best interests of the County. Conditional or qualified proposals are subject to rejection. The County reserves the right to reject the offer of an offeror who has previously failed to perform properly or to complete in a timely manner, contracts of a similar nature, or if investigation shows the offeror is unable to perform the requirements of the contract.

5. METHOD OF AWARD

This Informal Solicitation will be awarded to the “highest ranked offeror(s)”.

6. MINORITY, FEMALE, DISABLED PERSON PROGRAM COMPLIANCE

Under County law, this solicitation is subject to the Montgomery County Code and the Montgomery County Procurement Regulations regarding participation in the Minority, Female, Disabled Person (MFD) Procurement Program. Further information regarding the County's MFD program is contained within this solicitation (see the provision entitled "Minority-Owned Business Addendum to the General Conditions of Contract between County and Contractor" and its companion document entitled "Minority, Female, and Disabled-Person Subcontractor Performance Plan").

7. MONTGOMERY COUNTY CODE AND PROCUREMENT REGULATIONS

The Montgomery County and Procurement Regulations are applicable to this solicitation and any contract awarded pursuant to this solicitation.

8. NAME AND SIGNATURE REQUIREMENTS FOR Proposals AND CONTRACTS

The correct and full legal business name of the entity involved must be used on proposals received and on contract(s) issued as a result of this solicitation. A trade name, i.e., a shortened or different name under which the firm does business, must not be used when the full legal name is different. Corporations must have names that comply with State law, which requires a suffix indicating the corporate status of that business (e.g., Inc., Incorporated, etc.). Trade names may be indicated by individuals or corporations with the individual or corporate name followed by "t/a" (trading as) or "d/b/a" (doing business as), respectively. The signature on the bid, contract, amendment, or related correspondence must conform to the following:

All signatures must be made by an authorized officer, partner, manager, member, or employee. The signing of an offer or a contract is a representation by the person signing that the person signing is authorized to do so on behalf of the offeror or contractor.

No proposals will be accepted unless submitted in ink or typewritten. Changes made to the prices prior to the opening must be done legibly and initialed by the offeror making the changes.

9. PROMPT PAYMENT DISCOUNT TERMS

Proposers please note: Prompt payment discounts will be considered in the evaluation of your proposal if the discount on payments is not conditioned on payment being made in less than thirty (30) days from receipt of invoice.

10. OFFERORS PAYMENT TERMS

The County will reject as non-responsive a proposal under this Informal Solicitation, which is conditioned on payment of proper invoices in less than thirty (30) days. However, this does not preclude an offeror from offering a prompt payment discount for payment of invoices in less than thirty (30) days.

11. QUALIFICATION OF OFFERORS

Offerors may be required to furnish satisfactory evidence that they are qualified dealers or manufacturers of the items listed, or are regularly engaged in performing the services on which they are submitting a proposal, and in both cases maintain a regularly established place of business. An authorized representative of the County may visit and inspect any prospective Contractor's plant, manufacturing facility or place of business, etc. where the goods, services or construction are performed to determine ability, capacity, reliability, financial stability, and other factors necessary to perform the contract.

12. PROPOSAL PREPARATION EXPENSES

All costs incurred in the preparation and submission of proposals will be borne by the offeror and shall not be incurred in anticipation of receiving reimbursement from the County.

SECTION B. GENERAL CONDITIONS OF CONTRACT BETWEEN COUNTY & CONTRACTOR

1. ACCOUNTING SYSTEM AND AUDIT, ACCURATE INFORMATION

The contractor certifies that all information the contractor has provided or will provide to the County is true and correct and can be relied upon by the County in awarding, modifying, making payments, or taking any other action with respect to this contract including resolving claims and disputes. Any false or misleading information is a ground for the County to terminate this contract for cause and to pursue any other appropriate remedy. The contractor certifies that the contractor's accounting system conforms with generally accepted accounting principles, is sufficient to comply with the contract's budgetary and financial obligations, and is sufficient to produce reliable financial information.

The County may examine the contractor's and any first tier subcontractor's records to determine and verify compliance with the contract and to resolve or decide any claim or dispute arising under this contract. The contractor and any first tier subcontractor must grant the County access to these records at all reasonable times during the contract term and for 3 years after final payment. If the contract is supported to any extent with federal or state funds, the appropriate federal or state authorities may also examine these records. The contractor must include the preceding language of this paragraph in all first-tier subcontracts.

2. AMERICANS WITH DISABILITIES ACT

The contractor agrees to comply with the nondiscrimination requirements of Titles II and III, and other provisions, of the Americans with Disabilities Act of 1990, Pub. Law 101-336, and ADA Amendments Act of 2008, Pub. Law 110-325, as amended, currently found at 42 U.S.C., § 12101, et seq., and 47 U.S.C., ch. 5.

3. APPLICABLE LAWS

This contract must be construed in accordance with the laws and regulations of Maryland and Montgomery County. The Montgomery County Procurement Regulations are incorporated by reference into, and made a part of, this contract. In the case of any inconsistency between this contract and the Procurement Regulations, the Procurement Regulations govern. The contractor must, without additional cost to the County, pay any necessary fees and charges, obtain any necessary licenses and permits, and comply with applicable federal, state and local laws, codes and regulations. Through signature of this contract, the contractor certifies that the contractor has filed an initial statement with the Maryland State Board of Elections in compliance with MD Code Ann., Election Law, §14-104(b)(1), or is not required to file an initial statement as per MD Code Ann., Election Law, §14-104(c)(2).

For purposes of litigation involving this contract, except for contract Disputes discussed in paragraph 8 below, exclusive venue and jurisdiction must be in the Circuit Court for Montgomery County, Maryland or in the District Court of Maryland for Montgomery County.

The County's prevailing wage law, as found at §11B-33C of the County Code, applies to certain construction and mechanical systems service contracts. To the extent applicable, the County's prevailing wage requirements are enumerated within this solicitation/contract in the "Prevailing Wage Requirements for Construction Contract Addendum to the General Conditions of Contract between County and Contractor." If applicable to this contract, the Addendum will be attached to the contract, and will be incorporated herein by reference, and made a part thereof.

Furthermore, certain non-profit and governmental entities may purchase supplies and services, similar in scope of work and compensation amounts provided for in a County contract, using their own contract and procurement laws and regulations, pursuant to the Md. State Finance and Procurement Article, Section 13-101, et. seq.

Contractor and all of its subcontractors must comply with the provisions of County Code §11B-35A and must not retaliate against a covered employee who discloses an illegal or improper action described in §11B-35A. Furthermore, an aggrieved covered employee under §11B-35A is a third-party beneficiary under this Contract, who may by civil action recover compensatory damages including interest and reasonable attorney's fees, against the contractor or one of its subcontractors for retaliation in violation of that Section.

The contractor agrees to comply with the requirements of the Displaced Service Workers Protection Act, which appears in County Code, Chapter 27, Human Rights and Civil Liberties, Article X, Displaced Service Workers Protection Act, §§ 27-64 through 27-66.

Montgomery County's Earned Sick and Safe Leave Law, found at Sections 27-76 through 27-82 of the County Code, became effective October 1, 2016. An employer doing business in the County, as defined under the statute, must comply with this law. This includes an employer vendor awarded a

County contract. A vendor may obtain information regarding this law at http://www.montgomerycountymd.gov/humanrights/.

4. ASSIGNMENTS AND SUBCONTRACTS

The contractor must not assign or transfer this contract, any interest herein or any claim hereunder, except as expressly authorized in writing by the Director, Office of Procurement. Unless performance is separately and expressly waived in writing by the Director, Office of Procurement, an assignment does not release the contractor from responsibility for performance of this contract. Unless otherwise provided in the contract, the contractor may not contract with any other party for furnishing any of the materials or services herein contracted for without the written approval of the Director, Office of Procurement. Any subcontract for any work hereunder must comport with the terms of this Contract and County law, and must include any other terms and conditions that the County deems necessary to protect its interests. The contractor must not employ any subcontractor that is a debarred or suspended person under County Code §11B-37. The contractor is fully responsible to the County for the acts and omissions of itself, its subcontractors and any persons either directly or indirectly employed by them. Nothing contained in the contract documents shall create any contractual relation between any subcontractor and the County, and nothing in the contract documents is intended to make any subcontractor a beneficiary of the contract between the County and the contractor.

5. CHANGES

The Director, Office of Procurement, may unilaterally change the work, materials and services to be performed. The change must be in writing and within the general scope of the contract. The contract will be modified to reflect any time or money adjustment the contractor is entitled to receive. Contractor must bring to the Contract Administrator, in writing, any claim about an adjustment in time or money resulting from a change, within 30 days from the date the Director, Office of Procurement, issued the change in work, or the claim is waived. Any failure to agree upon a time or money adjustment must be resolved under the "Disputes" clause of this contract. The contractor must proceed with the prosecution of the work as changed, even if there is an unresolved claim. No charge for any extra work, time or material will be allowed, except as provided in this section.

6. CONTRACT ADMINISTRATION

A. The contract administrator, subject to paragraph B below, is the Department representative designated by the Director, Office of Procurement, in writing and is authorized to:

1) serve as liaison between the County and the contractor;

2) give direction to the contractor to ensure satisfactory and complete performance;

3) monitor and inspect the contractor's performance to ensure acceptable timeliness and quality;

4) serve as records custodian for this contract, including wage and prevailing wage requirements;

5) accept or reject the contractor's performance;

6) furnish timely written notice of the contractor's performance failures to the Director, Office of Procurement, and to the County Attorney, as appropriate;

7) prepare required reports;

8) approve or reject invoices for payment;

9) recommend contract modifications or terminations to the Director, Office of Procurement;

10) issue notices to proceed; and

11) monitor and verify compliance with any MFD Performance Plan.

B. The contract administrator is NOT authorized to make determinations (as opposed to recommendations) that alter, modify, terminate or cancel the contract, interpret ambiguities in contract language, or waive the County's contractual rights.

7. COST & PRICING DATA

Chapter 11B of the County Code and the Montgomery County Procurement Regulations require that cost & pricing data be obtained from proposed awardees/contractors in certain situations. The contractor guarantees that any cost & pricing data provided to the County will be accurate and complete. The contractor grants the Director, Office of Procurement, access to all books, records, documents, and other supporting data in order to permit adequate evaluation of the contractor's proposed price(s). The contractor also agrees that the price to the County, including profit or fee, may, at the option of the County, be reduced to the extent that the price was based on inaccurate, incomplete, or noncurrent data supplied by the contractor.

8. DISPUTES

Any dispute arising under this contract that is not disposed of by agreement must be decided under the Montgomery County Code and the Montgomery County Procurement Regulations. Pending final resolution of a dispute, the Contractor must proceed diligently with contract performance. Subject to subsequent revocation or alteration by the Director, Office of Procurement, the head of the County department, office or agency ("Department Head") of the contract administrator is the designee of the Director, Office of Procurement, for the purpose of dispute resolution. The Department Head, or his/her designee, must forward to the Director, Office of Procurement, a copy of any written resolution of a dispute. The Department Head may delegate this responsibility to another person (other than the contract administrator). A contractor must notify the contract administrator of a claim in writing, and must attempt to resolve a claim with the contract administrator prior to filing a dispute with the Director, Office of Procurement or designee. The contractor waives any dispute or claim not made in writing and received by the Director, Office of Procurement, within 30 days of the event giving rise to the dispute or claim, whether or not the contract administrator has responded to a written notice of claim or resolved the claim. The Director, Office of Procurement, must dismiss a dispute that is not timely filed. A dispute must be in writing, for specific relief, and any requested relief must be fully supported by affidavit of all relevant calculations, including cost and pricing information, records, and other information. At the County's option, the contractor agrees to be made a party to any related dispute involving another contractor.

9. DOCUMENTS, MATERIALS, AND DATA

All documents, materials, or data developed as a result of this contract are the County's property. The County has the right to use and reproduce any documents, materials, and data, including confidential information, used in the performance of, or developed as a result of, this contract. The County may use this information for its own purposes, including reporting to state and federal agencies. The contractor warrants that it has title to or right of use of all documents, materials or data used or developed in connection with this contract. The contractor must keep confidential all documents, materials, and data prepared or developed by the contractor or supplied by the County.

10. DURATION OF OBLIGATION

The contractor agrees that all of contractor's obligations and warranties, including all requirements imposed by the Minority Owned Business Addendum to these General Conditions, if any, which directly or indirectly are intended by their nature or by implication to survive contractor performance, do survive the completion of performance, termination for default, termination for convenience, or termination by mutual consent of the contract.

11. ENTIRE AGREEMENT

There are no promises, terms, conditions, or obligations other than those contained in this contract. This contract supersedes all communications, representations, or agreements, either verbal or written, between the parties hereto, with the exception of express warranties given to induce the County to enter into the contract.

12. ETHICS REQUIREMENTS/POLITICAL CONTRIBUTIONS

The contractor must comply with the ethics provisions contained in Chapters 11B and 19A, Montgomery County Code, which include the following:

a) a prohibition against making or offering to make certain gifts. Section 11B-51(a).

b) a prohibition against kickbacks. Section 11B-51(b).

c) a prohibition against a person engaged in a procurement from employing or offering to employ a public employee. Section 11B-52(a).

d) a prohibition against a contractor that is providing a recommendation to the County from assisting another party or seeking to obtain an economic benefit beyond payment under the contract. Section 11B-52(b).

e) a restriction on the use of confidential information obtained in performing a contract. Section 11B-52(c).

f) a prohibition against contingent fees. Section 11B-53.

Furthermore, the contractor specifically agrees to comply with Sections 11B-51, 11B-52, 11B-53, 19A-12, and/or 19A-13 of the Montgomery County Code. In addition, the contractor must comply with the political contribution reporting requirements currently codified under the Election Law at Md. Code Ann., Title 14.

13. GUARANTEE

A. Contractor guarantees for one year from acceptance, or for a longer period that is otherwise expressly stated in the County’s written solicitation, all goods, services, and construction offered, including those used in the course of providing the goods, services, and/or construction. This includes a guarantee that all products offered (or used in the installation of those products) carry a guarantee against any and all defects for a minimum period of one year from acceptance, or for a longer period stated in the County’s written solicitation. The contractor must correct any and all defects in material and/or workmanship that may appear during the guarantee period, or any defects that occur within one (1) year of acceptance even if discovered more than one (1) year after acceptance, by repairing, (or replacing with new items or new materials, if necessary) any such defect at no cost to the County and to the County’s satisfaction.

C. Should a manufacturer's or service provider’s warranty or guarantee exceed the requirements stated above, that guarantee, or warranty will be the primary one used in the case of defect. Copies of manufacturer's or service provider’s warranties must be provided upon request.

D. All warranties and guarantees must be in effect from the date of acceptance by the County of the goods, services, or construction.

E. The contractor guarantees that all work shall be accomplished in a workmanlike manner, and the contractor must observe and comply with all Federal, State, County and local laws, ordinances and regulations in providing the goods, and performing the services or construction.

F. Goods and materials provided under this contract must be of first quality, latest model and of current manufacture, and must not be of such age or so deteriorated as to impair their usefulness or safety. Items that are used, rebuilt, or demonstrator models are unacceptable, unless specifically requested by the County in the Specifications.

14. HAZARDOUS AND TOXIC SUBSTANCES

Manufacturers and distributors are required by federal "Hazard Communication” provisions (29 CFR 1910.1200), and the Maryland "Access to Information About Hazardous and Toxic Substances" Law, to label each hazardous material or chemical container, and to provide Material Safety Data Sheets to the purchaser. The contractor must comply with these laws and must provide the County with copies of all relevant documents, including Material Safety Data Sheets, prior to performance of work or contemporaneous with delivery of goods.

15. HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) COMPLIANCE

In addition to the provisions stated above in Section 3. “Applicable Laws,” contractor must comply with all requirements in the federal Health Insurance Portability and Accountability Act (HIPAA), to the extent that HIPAA is applicable to this contract. Furthermore, contractor must enter into the County’s standard Business Associate Agreement or Qualified Service Organization Agreement when contractor or the County, as part of this contract, may use or disclose to one another, to the individual whose health information is at issue, or to a third-party, any protected health information that is obtained from, provided to, made available to, or created by, or for, the contractor or the County.

16. IMMIGRATION REFORM AND CONTROL ACT

The contractor warrants that both the contractor and its subcontractors do not, and shall not, hire, recruit or refer for a fee, for employment under this contract or any subcontract, an alien while knowing the alien is an unauthorized alien, or any individual without complying with the requirements of the federal Immigration and Nationality laws, including any verification and record keeping requirements. The contractor further assures the County that, in accordance with those laws, it does not, and will not, discriminate against an individual with respect to hiring, recruitment, or referral for a fee, of an individual for employment or the discharge of an individual from employment, because of the individual's national origin or, in the case of a citizen or prospective citizen, because of the individual's citizenship status.

17. INCONSISTENT PROVISIONS

Notwithstanding any provisions to the contrary in any contract terms or conditions supplied by the contractor, this General Conditions of Contract document supersedes the contractor's terms and conditions, in the event of any inconsistency.

18. INDEMNIFICATION

The contractor is responsible for any loss, personal injury, death and any other damage (including incidental and consequential) that may be done or suffered by reason of the contractor's negligence or failure to perform any contractual obligations. The contractor must indemnify and save the County harmless from any loss, cost, damage and other expenses, including attorney's fees and litigation expenses, suffered or incurred due to the contractor's negligence or failure to perform any of its contractual obligations. If requested by the County, the contractor must defend the County in any action or suit brought against the County arising out of the contractor's negligence, errors, acts or omissions under this contract. The negligence of any agent, subcontractor or employee of the contractor is deemed to be the negligence of the contractor. For the purposes of this paragraph, County includes its boards, agencies, agents, officials and employees.

19. INDEPENDENT CONTRACTOR

The contractor is an independent contractor. The contractor and the contractor's employees or agents are not agents of the County.

20. INSPECTIONS

The County has the right to monitor, inspect and evaluate or test all supplies, goods, services, or construction called for by the contract at all reasonable places (including the contractor's place of business) and times (including the period of preparation or manufacture).

21. INSURANCE

Prior to contract execution by the County, the proposed awardee/contractor must obtain at its own cost and expense the minimum insurance specified in the applicable table (See Tables A and B) or attachment to these General Conditions, with one or more insurance company(s) licensed or qualified to do business in the State of Maryland and acceptable to the County's Division of Risk Management. The minimum limits of coverage listed shall not be construed as the maximum as required by contract or as a limitation of any potential liability on the part of the proposed awardee/contractor to the County, nor shall failure by the County to request evidence of this insurance in any way be construed as a waiver of proposed awardee/contractor's obligation to provide the insurance coverage specified. Contractor must keep this insurance in full force and effect during the term of this contract, including all extensions. Unless expressly provided otherwise, Table A is applicable to this contract. The insurance must be evidenced by one or more Certificate(s) of Insurance and, if requested by the County, the proposed awardee/contractor must provide a copy of any and all insurance policies to the County. At a minimum, the proposed awardee/contractor must submit to the Director, Office of Procurement, one or more Certificate(s) of Insurance prior to award of this contract, and prior to any contract modification extending the term of the contract, as evidence of compliance with this provision. The contractor's insurance must be primary. Montgomery County, MD, including its officials, employees, agents, boards, and agencies, must be named as an additional insured on all liability policies. Contractor must provide to the County at least 30 days written notice of a cancellation of, or a material change to, an insurance policy. In no event may the insurance coverage be less than that shown on the applicable table, attachment, or contract provision for required insurance. After consultation with the Department of Finance, Division of Risk Management, the Director, Office of Procurement, may waive the requirements of this section, in whole or in part.

Please disregard TABLE A. and TABLE B., if they are replaced by the insurance requirements as stated in an attachment to these General Conditions of Contract between County and Contractor.

TABLE A. INSURANCE REQUIREMENTS

(See Paragraph #21 under the General Conditions of Contract between County and Contractor)

CONTRACT DOLLAR VALUES (IN $1,000's)				
	Up to 50	Up to 100	Up to 1,000	Over 1,000
Workers Compensation (for contractors with employees)				
Bodily Injury by				
Accident (each)	100	100	100	See Attachment
Disease (policy limits)	500	500	500	

CONTRACT DOLLAR VALUES (IN $1,000’s)				
	Up to 50	Up to 100	Up to 1,000	Over 1,000
Disease (each employee)	100	100	100	
Commercial General Liability	300	500	1,000	See Attachment
for bodily injury and property damage per occurrence, including contractual liability, premises and operations, and independent contractors				
Minimum Automobile Liability (including owned, hired and non-owned automobiles) Bodily Injury				
each person	100	250	500	See Attachment
each occurrence	300	500	1,000	
Property Damage				
each occurrence	300	300	300	
Professional Liability*	250	500	1,000	See Attachment
for errors, omissions and negligent acts, per claim and aggregate, with one-year discovery period and maximum deductible of $25,000				
Certificate Holder Montgomery County Maryland (Contract #) Office of Procurement 27 Courthouse Square, Suite 330, Rockville, MD 20850				
*Professional services contracts only				

TABLE B. INSURANCE REQUIREMENTS
(See Paragraph #21 under the General Conditions of Contract between County and Contractor)

CONTRACT DOLLAR VALUES (IN $1,000’s)				
	Up to 50	Up to 100	Up to 1,000	Over 1,000
Commercial General Liability minimum combined single limit for bodily injury and property damage per occurrence, including contractual liability, premises and operations, independent contractors, and product liability	300	500	1,000	See Attachment
Certificate Holder Montgomery County Maryland (Contract #) Office of Procurement 27 Courthouse Square, Suite 330, Rockville, MD 20850				

22. INTELLECTUAL PROPERTY APPROVAL AND INDEMNIFICATION – INFRINGEMENT

If contractor will be preparing, displaying, publicly performing, reproducing, or otherwise using, in any manner or form, any information, document, or material that is subject to a copyright, trademark, patent, or other property or privacy right, then contractor must: obtain all necessary licenses, authorizations, and approvals related to its use; include the County in any approval, authorization, or license related to its use; and indemnify and hold harmless the County related to contractor's alleged infringing or otherwise improper or unauthorized use. Accordingly, the contractor must protect, indemnify, and hold harmless the County from and against all liabilities, actions, damages, claims, demands, judgments, losses, costs, expenses, suits, or actions, and attorneys' fees and the costs of the defense of the County, in any suit, including appeals, based upon or arising out of any allegation of infringement, violation, unauthorized use, or conversion of any patent, copyright, trademark or trade name, license, proprietary right, or other related property or privacy interest in connection with, or as a result of, this contract or the performance by the contractor of any of its activities or obligations under this contract.

23. INFORMATION SECURITY

A. Protection of Personal Information by Government Agencies:

In any contract under which Contractor is to perform services and the County may disclose to Contractor personal information about an individual, as defined by State law, Contractor must implement and maintain reasonable security procedures and practices that: (a) are appropriate to the nature of the personal information disclosed to the Contractor; and (b) are reasonably designed to help protect the personal information from unauthorized access, use, modification, disclosure, or destruction. Contractor's requirement to implement and maintain reasonable security practices and procedures must include requiring any third-party to whom it discloses personal information that was originally disclosed to Contractor by the County to also implement and maintain reasonable security practices and procedures related to protecting the personal information. Contractor must notify the County of a breach of the security of a system if the unauthorized acquisition of an individual's personal information has occurred or is reasonably likely to occur, and also must share with the County all information related to the breach. Contractor must provide the above notification to the County as soon as reasonably practicable after Contractor discovers or is notified of the breach of the security of a system. Md. Code Ann., State Gov't. § 10-1301 through 10-1308 (2013).

B. Payment Card Industry Compliance:

In any contract where the Contractor provides a system or service that involves processing credit card payments (a "Payment Solution"), the Payment Solution must be Payment Card Industry Data Security Standard Compliant ("PCI-DSS Compliant"), as determined and verified by the Department of Finance, and must (1) process credit card payments through the use of a Merchant ID ("MID") obtained by the County's Department of Finance by and in the name of the County as merchant of record, or (2) use a MID obtained by and in the name of the Contractor as merchant of record.

24. NON-CONVICTION OF BRIBERY

The contractor hereby declares and affirms that, to its best knowledge, none of its officers, directors, or partners or employees directly involved in obtaining contracts has been convicted of bribery, attempted bribery, or conspiracy to bribe under any federal, state, or local law.

25. NON-DISCRIMINATION IN EMPLOYMENT

The contractor agrees to comply with the non-discrimination in employment policies and/ or provisions prohibiting unlawful employment practices in County contracts as required by Section 11B 33 and Section 27 19 of the Montgomery County Code, as well as all other applicable state and federal laws and regulations regarding employment discrimination.

The contractor assures the County that, in accordance with applicable law, it does not, and agrees that it will not, discriminate in any manner on the basis of race, color, religious creed, ancestry, national origin, age, sex, marital status, disability, or sexual orientation.

The contractor must bind its subcontractors to the provisions of this section.

26. PAYMENT AUTHORITY

No payment by the County may be made, or is due, under this contract, unless funds for the payment have been appropriated and encumbered by the County. Under no circumstances will the County pay the contractor for legal fees, late fees, or shipping fees that are not provided for in the contract. The contractor must not proceed to perform any work (provide goods, services, or construction) prior to receiving written confirmation that the County has appropriated and encumbered funds for that work. If the contractor fails to obtain this verification from the Office of Procurement prior to performing work, the County has no obligation to pay the contractor for the work.

If this contract provides for an additional contract term for contractor performance beyond its initial term, continuation of contractor’s performance under this contract beyond the initial term is contingent upon, and subject to, the appropriation of funds and encumbrance of those appropriated funds for payments under this contract. If funds are not appropriated and encumbered to support continued contractor performance in a subsequent fiscal period, contractor’s performance must end without further notice from, or cost to, the County. The contractor acknowledges that the County Executive has no obligation to recommend, and the County Council has no obligation to appropriate, funds for this contract in subsequent fiscal years. Furthermore, the County has no obligation to encumber funds to this contract in subsequent fiscal years, even if appropriated funds may be available. Accordingly, for each subsequent contract term, the contractor must not undertake any performance under this contract until the contractor receives a purchase order or contract amendment from the County that authorizes the contractor to perform work for the next contract term.

27. P-CARD OR SUA PAYMENT METHODS

The County is expressly permitted to pay the vendor for any or all goods, services, or construction under the contract through either a procurement card (“P-card”) or a Single Use Account (“SUA”) method of payment, if the contractor accepts the noted payment method from any other person. In that event, the County reserves the right to pay any or all amounts due under the contract by using either a p-card (except when a purchase order is required) or a SUA method of payment, and the contractor must accept the County’s p-card or a SUA method of payment, as applicable. Under this paragraph, contractor is prohibited from charging or requiring the County to pay any fee, charge, price, or other obligation for any reason related to or associated with the County’s use of either a p-card or a SUA method of payment.

28. PERSONAL PROPERTY

All furniture, office equipment, equipment, vehicles, and other similar types of personal property specified in the contract, and purchased with funds provided under the contract, become the property of the County upon the end of the contract term, or upon termination or expiration of this contract, unless expressly stated otherwise.

29. TERMINATION FOR DEFAULT

The Director, Office of Procurement, may terminate the contract in whole or in part, and from time to time, whenever the Director, Office of Procurement, determines that the contractor is:

a) defaulting in performance or is not complying with any provision of this contract;

b) failing to make satisfactory progress in the prosecution of the contract; or

c) endangering the performance of this contract.

The Director, Office of Procurement, will provide the contractor with a written notice to cure the default. The termination for default is effective on the date specified in the County's written notice. However, if the County determines that default contributes to the curtailment of an essential service or poses an immediate threat to life, health, or property, the County may terminate the contract immediately upon issuing oral or written notice to the contractor without any prior notice or opportunity to cure. In addition to any other remedies provided by law or the contract, the contractor must compensate the County for additional costs that foreseeably would be incurred by the County, whether the costs are actually incurred or not, to obtain substitute performance. A termination for default is a termination for convenience if the termination for default is later found to be without justification.

30. TERMINATION FOR CONVENIENCE

This contract may be terminated by the County, in whole or in part, upon written notice to the contractor, when the County determines this to be in its best interest. The termination for convenience is effective on the date specified in the County's written notice. Termination for convenience may entitle the contractor to payment for reasonable costs allocable to the contract for work or costs incurred by the contractor up to the date of termination. The contractor must not be paid compensation as a result of a termination for convenience that exceeds the amount encumbered to pay for work to be performed under the contract.

31. TIME

Time is of the essence.

32. WORK UNDER THE CONTRACT

Contractor must not commence work under this contract until all conditions for commencement are met, including execution of the contract by both parties, compliance with insurance requirements, encumbrance of funds, and issuance of any required notice to proceed.

33. WORKPLACE SAFETY

The contractor must ensure adequate health and safety training and/or certification, and must comply with applicable federal, state and local Occupational Safety and Health laws and regulations.

THIS FORM MUST NOT BE MODIFIED WITHOUT THE PRIOR APPROVAL OF THE OFFICE OF THE COUNTY ATTORNEY.
Rev. 07/2022

SECTION C. SPECIAL TERMS AND CONDITIONS

1. GENERAL CONDITIONS

The General Conditions of Contract between County & Contractor (Section B) are incorporated and made part of this Informal Solicitation and any resultant contract, except that the insurance requirements listed in Provision 21 are replaced by the Mandatory Insurance Requirements listed in Attachment B.

2. COMPENSATION

The County will pay the Contractor on a monthly basis, within 30 days after the County's receipt and acceptance of an invoice submitted by the contractor and in a form approved by the County.

3. CONTRACT ADMINISTRATOR

The Contract Administrator, or designee, is responsible for inspecting all work and authorizing payment upon acceptance.

The designated Contract Administrator for the Department/Office of Environmental Protection is Scott Faunce.

4. CONTRACT TERM

The term of the contract is for **one** year from the date of signature by the Director, Office of Procurement. Before the contract term ends, the Director may (but is not required to) renew this contract, if the Director determines that renewal is in the best interests of the County. The Contractor's satisfactory performance does not guarantee renewal of this Contract. The Director may exercise this option to renew for **two** additional one-year periods. The contract will automatically terminate once $99,999 has been spent.

5. ANNUAL PRICE ADJUSTMENT

Prices quoted are firm for a period of one year after execution of the contract. Any request for a price adjustment after this one-year period, is subject to the following:

A. Approval or rejection by the Director, Office of Procurement or designee.

B. **Must be submitted in writing to the Director, Office of Procurement, and accompanied by supporting documentation justifying the Contractor's request.** A request for any price adjustment may not be approved unless the contractor submits to the County sufficient justification to support that the Contractor's request is based on its net increase in costs in delivering the goods/services to the County under the contract terms.

C. Must be submitted sixty (60) days prior to the contact expiration date, if the contract is being amended.

D. May not be approved in an amount that exceeds the annual percentage change of the Consumer Price Index (CPI) for the twelve-month period immediately prior to the date of the request. **The request must not exceed the CPI for all urban consumers issued for the Washington-Arlington-Alexandria, DC-VA-MD-WV Metropolitan area by the United States Department of Labor, Bureau of Labor Statistics for ALL ITEMS.** The County will approve only one price adjustment for each contract term, if a price adjustment is approved.

E. Should be effective sixty (60) days from the date of receipt of the contractor's request.

F. Must be executed by written contract amendment.

6. ETHICS

As a result of being awarded a contract resulting from this solicitation, the successful contractor may be ineligible for the award of related contracts. In this regard, Montgomery County Code Sections 11B-52 (b) and (c) state the following:

> *A contract providing an analysis or recommendation to the County concerning a particular matter must not, without first obtaining the written consent of the Chief Administrative Officer:*
>
> *[…]*
>
> *b) Assist another part in the matter or another person if the person has a direct and substantial interest in the matter; or*
>
> *c) Seek or obtain an economic benefit from the matter in addition to payment to the contractor by the County.*

7. INDEPENDENT CONTRACTOR/CONTRACTOR CONDUCT

A. For the purposes of this Contract, the Contractor’s personnel and the personnel retained by any approved subcontractor engaged by the Contractor are the employees, consultants, workers and contractors of the Contractor or subcontractor, as applicable. The Contractor’s personnel and the personnel of any subcontractor engaged by the Contractor are not employees of Montgomery County. The Contractor’s personnel and the personnel of any subcontractor engaged by the Contractor must not represent themselves as an employee of the County in their interaction with the public, other contractors, or County employees. In situations where the Contractor’s personnel or the personnel of any subcontractor engaged by the Contractor may be mistaken for a County employee, the Contractor’s personnel and the personnel of any subcontractor engaged by the Contractor must disclose that they are working under a County contract and that they are not a County employee. Persons assigned to work for the County under this Contract must not set policies for the County or independently interpret County policies.

B. The Contractor must provide administrative oversight for, and coordinate the recruitment, hiring/subcontracting, termination and placement of, qualified individuals who will provide the services as stipulated in this Contract. The Contractor must also provide overall supervision, control over, and direction of all personnel who work under this Contract in the provision of the services described in this Contract.

C. The Contractor and any subcontractor engaged by the Contractor must abide by all federal, state and local labor laws and regulations and all applicable federal, state, and local tax laws and regulations in the hiring and management of all personnel employed or retained to provide services to the County under this Contract. For purposes of this Contract, “personnel” means the employees, consultants, contractors, or other worker retained by the Contractor or any subcontractor engaged by the Contractor to provide the services under this Contract.

D. The Contractor or any subcontractor engaged by the Contractor, as applicable, must be responsible for all taxes, as well as other obligations or benefits related to its workers, including F.I.C.A., federal, and state withholdings, unemployment, and workers’ compensation for persons who work for the Contractor or the subcontractor engaged by the Contractor under this Contract in the provision of the services described in this Contract.

E. The Contractor’s personnel and the personnel of any subcontractor engaged by the Contractor to provide services under this Contract are not entitled to the use of, and must not use, County vehicles.

F. The Contractor's personnel and the personnel of any subcontractor engaged by the Contractor are not entitled to benefits available to County employees, including but not limited to credit union membership, administrative leave, access to deferred compensation benefits, affirmative action initiatives, personnel services, employee training, and other Count employee benefits.

G. The Contractor or any subcontractor engaged by the Contractor, as applicable, is solely responsible for all costs or expenses related to personnel costs of its personnel, including those related to wages, benefits, training, fringe benefits and paid leave.

H. Upon request by the County, the Contractor must provide the County with access to any materials, records or reports produced by any of the Contractor's or the subcontractor's personnel, including, but not limited to pamphlets, surveys, evaluations, training materials and customized software. Any materials, records, or reports produced by the Contractor's personnel or the personnel of any subcontractor engaged by the Contractor performing work under this Contract are the County's property.

I. The County will own all work products produced by the Contractor or any subcontractor engaged by the Contractor to provide services under this Contract when those work products are produced: 1) while assigned to the County Contract; 2) during the time and/or in the space used for County contract work; and 3) within the general scope of work assigned under the Contract. The County has the sole right to own, license, sell or use such work products. The Contractor's or subcontractor's personnel, and the personnel of any contractor or subcontractor engaged by the Contractor will have no such rights to work products produced for the County.

J. All original content and work products developed under this Contract, including, but not limited to, graphics, data, content, information, photos and other products developed as a result of the work performed under the Contract are the sole and exclusive property of Montgomery County, Maryland; are for the exclusive, unlimited use of the County; and must not be used or distributed by the Contractor without prior written permission of the County.

K. The Contractor must: ensure that any third-party references, graphics, or resource materials used are royalty-free; have licenses for use of such materials when applicable; and properly credit such materials to their source when so required by the source.

L. The Contractor must not use, publish, or release any information relative to the Contract without the prior written approval of the Contract Administrator, including, but not limited to, mailing lists, brochures, pamphlets, catalogs, data, drawings, photos, reports, video or media clips, descriptions and correspondence. Any such information generated by the Contractor specifically for use in performing the work under the Contract must not be issued, published, or released by the Contractor without prior written consent of the Contract Administrator.

8. INVOICES

All true and correct invoices and all inquiries regarding payment are to be sent to DEP.Invoice@montgomerycountymd.gov. **Failure to promptly comply with this requirement must delay payment**.

9. PURCHASE OF GOODS BY NON-PROFIT ORGANIZATIONS

Pursuant to the requirements set forth in the Montgomery County Code, Chapter 11B-49, the Contractor agrees to extend the same terms, conditions, and prices for the goods provided by the Contractor pursuant to this contract to those Non-Profit organizations which may need the goods in order to perform a contract with the County. Non-Profit Organizations are defined as those organizations that are exempt from taxation under Section 501(c)(3) of the Internal Revenue Code but are not defined as a "public entity" under subsection (n) of Chapter 11B-1 of the Montgomery County Code.

10. TRAVEL TIME - Not Applicable

~~No payment for travel time to or from a job site shall be charged. Charges begin when the Contractor arrives at each job site and end when the Contractor leaves each job site. The Project Coordinator or Contract Administrator will verify time records.~~

SECTION D. SCOPE OF SERVICES

1. BACKGROUND

   A. This project involves the remediation of PDF documents to ensure full compliance with the Web Content Accessibility Guidelines (WCAG) 2.1 Level AA. The requirement is to make all PDF content accessible to individuals with disabilities, including those using assistive technologies such as screen readers.

   B. The United State Department of Justice approved and published a rule updating the ADA Title II regulation in the Federal Register requiring US state and local jurisdictions to comply with the WCAG 2.1 Level AA. Montgomery County is required to comply with the new Title II ADA regulation by 4/24/2026.

   C. DEP must remediate existing PDFs to comply with the WCAG 2.1 Level AA by 4/24/2026.

   D. Objectives

      a. Remediate PDF documents to meet WCAG 2.1 Level AA standards.

      b. Ensure compatibility with assistive technologies (e.g., JAWS, NVDA, VoiceOver).

      c. Provide accessible, tagged PDFs that maintain the original document’s visual integrity.

2. SCOPE OF SERVICES

   A. Document Assessment

      a. Review and assess all provided PDF documents. (1,500 estimated total pages)

      b. Identify accessibility issues and remediation requirements.

      c. Provide a report summarizing findings and estimated effort per document.

   B. PDF Remediation

      a. Apply proper tagging structure (headings, lists, tables, etc.).

      b. Add alternative text for all meaningful images and graphics.

      c. Ensure correct reading order and logical document structure.

      d. Remediate tables for accessibility (headers, scope, summaries).

      e. Ensure form fields are interactive and accessible (if applicable).

      f. Remove or remediate inaccessible elements (e.g., scanned text without OCR).

      g. Ensure color contrast and font readability.

      h. Remediated documents must comply with WCAG 2.1 Level AA standards (Attachment F).

C. Quality Assurance

a. Conduct internal QA using assistive technologies such as screen readers and accessibility checkers e.g., Adobe Acrobat Pro, JAWS, NVDA, VoiceOver, PAC2024).

b. Validate compliance with WCAG 2.1 Level AA (Attachment F) and Portable Document Format/Universal Accessibility PDF/UA standards (Attachment F).

c. Provide a compliance report for each remediated document.

D. Deliverables

a. Fully remediated and accessible PDF files.

b. Accessibility compliance report from PAC 2024 needs to be included for each document.

c. Bi-weekly summary report of all remediated documents and compliance status.

E. Acceptance Criteria

a. All PDFs pass accessibility checks using Adobe Acrobat Pro and PAC 2024.

b. Documents are usable with major screen readers (e.g., JAWS, NVDA, VoiceOver).

c. DEP approval of final deliverables.

d. The Contractor must guarantee their work. If corrections are needed, the Contractor must remediate all errors at no extra cost to the County.

3. CONTRACTOR RESPONSIBILITIES

a. The Contractor must maintain its business in "good standing" with the State of Maryland Department of Assessments and Taxation Business Services, https://dat.maryland.gov/businesses/Pages/default.aspx, at all times during the performance of the Contract.

b. The Contractor must maintain and update, as applicable, the Contractor's information in the County's Central Vendor Registration System (CVRS) at https://www.montgomerycountymd.gov/PRO/news/NewCVRS.html within 15 days of any changes. This includes any Automated Clearinghouse (ACH) changes for payment deposits that can only be updated through the CVRS system by the Contractor.

c. The Contractor must notify the County within 15 days of any changes in the company name (including "dba" changes), address, and/or Tax ID changes. The e-mail to submit this information is DEP.Procurements@montgomerycountymd.gov.

d. The Contractor must furnish a current Certificate of Insurance (COI) that complies with the requirements in Attachment C to this solicitation before execution of the Contract. The ACORD form, or equivalent, must be provided to the County for Risk Management review and approval. COI renewals must be submitted within 15 days of expiration to DEP.Procurements@montgomerycountymd.gov. If the Contractor's Certificate issuer permits, it is recommended that the Contractor add the DEP Procurements e-mail to a direct-distribute list so DEP will receive COI renewals directly from the broker.

e. The Contractor must notify the County of any key personnel changes a minimum of 15 business days before the change occurs.

f. The Contractor is responsible for the entire performance under the Contract regardless of whether the Contractor itself performs. The Contractor is the sole point of contact concerning the management of the Contract, including performance and payment issues. The Contractor is solely and completely responsible for adherence by the Contractor Parties to all applicable provisions of the Contract.

g. The Contractor is expected to be able to work closely with County staff.

4. COUNTY RESPONSIBILITIES

A. County will provide all source PDF files.

B. No redesign or content rewriting is required by the Contractor.

C. Documents are primarily in English, and no translation or localization services are required.

D. County subject matter experts will be available to answer questions from Contractor if required, including translation related questions.

5. CONTRACTOR'S QUALIFICATIONS

A. Contractor's focus must be solely on accessibility remediation of PDF documents.

B. Minimum of 5 years' experience providing PDF remediation services.

C. Prior experience providing remediation services for government organizations.

6. INFORMATION SECURITY

A. The Contractor must use commercially responsible efforts to ensure that the County's information resources, including electronic data assets, are protected from theft, unauthorized destruction, use, modification, or disclosure as deemed necessary under the County's Information Resources Security Procedure (AP 6-7) (Attachment G). To the extent the County has access to the County's network, the Contractor must adhere to the County's Information Resources Security Procedure (6-7). This document will be provided to the awardee.

SECTION E. METHOD OF AWARD/EVALUATION CRITERIA

1. PROCEDURES

A. Upon receipt of proposals, the Department of Environmental Protection will review and evaluate all proposals in accordance with the evaluation criteria listed below. Subject matter experts will also review for responsibility.

B. Vendor interviews will not be conducted.

C. The evaluation team will make its award recommendation of the highest ranked offeror based on the written score and its responsibility determination.

D. After the successful conclusion of negotiations, the using department will forward the Contract to the Director, Office of Procurement, which will execute the Contract.

2. EVALUATION CRITERIA

A. Written Evaluation Criteria

Written Proposals must specifically address:

a. Describe the software your firm uses to remediate and validate documents.

b. The County has created a OneDrive folder with files for remediation, if the Offeror has other options for how the County will submit documents for remediation and how the documents be returned, please describe it.

c. Explain your validation process.

d. Describe the screen reading technology and other software used to validate documents.

e. Describe the experience of your validators. (Resumes of up to two electronic pages per individual are acceptable).

f. Describe how your firm meets the five-year minimum experience requirement.

g. Describe prior experience providing remediation services for government organizations.

CRITERIA	POINTS
1. Written Proposal (Max 5 Electronic Pages – not including resumes)	25
2. Fee Schedule (Attachment A - Mandatory)	35
3. Remediation Documents - Accuracy and Compliance (Attachment D-Mandatory)	40
TOTAL	**100**

SECTION F. SUBMISSIONS

A. Offerors must submit their proposal in the format below. Written proposals will be evaluated on only material that is submitted. The offeror must submit sufficient information to enable the Evaluation Committee to evaluate the offeror's capabilities and experience. Proposals must include the following information:

1. A cover letter with a brief description of the business entity, including the offeror's name, address, telephone number, and email address.
2. Written Proposal as described in Section E.
3. The completed Acknowledgement Page of this solicitation, signed by a person authorized to bind the offeror to the proposal.
4. At least three references that may be contacted to attest to the quality and timeliness of the offeror's work of similar nature and scope as that required by the County in this solicitation. (Attachment C)
5. The offeror must submit the appropriate Wage Requirements Law forms (PMMD-177, see #3 below Web-links).
6. Minority, Female, Disabled Persons Subcontractor Performance Plan (PMMD-65, see #2 below Web-links).
7. Fee Schedule (Attachment A)
8. Three Sample Remediated documents (Attachment D)

WEB-LINKS FOR DOCUMENTS AND FORMS

1. County Vendor Registration System, https://www.montgomerycountymd.gov/vendorregistration.
2. Minority, Female, Disabled Person Subcontractor Performance Plan and Sample MFD Report of Payments Received, www.montgomerycountymd.gov/PRO/Resources/Files/SolForm/PMMD-65.pdf, www.montgomerycountymd.gov/PRO/Resources/Files/SolForm/PMMD-97.pdf.
3. Wage Requirements for Services Contracts Addendum and Wage Requirements Certification Form and 501(c)(3) Nonprofit Organization's Employee's Wage and Health Insurance Form, www.montgomerycountymd.gov/PRO/Resources/Files/SolForm/PMMD-177.pdf.

ATTACHMENT A,
FEE SCHEDULE

Cost Table	
Base Page Rate	$____________ Per Page
OR	
Base Hourly Rate Per Document	$____________ Per Document
OR HOURLY RATE BY STAFF LEVEL	
Position Title	**Rate**
	$____________ Hourly Rate Per Document
	$____________ Hourly Rate Per Document
	$____________ Hourly Rate Per Document
	$____________ Hourly Rate Per Document
	$____________ Hourly Rate Per Document
TOTAL COSTS: Based off an estimated 1,500 Total Pages (Using one rate method above)	$____________ For Estimated 1,500 pages

1. Applicants may choose to submit their costs by either the base page rate, the base hourly rate, or if utilizing multiple levels of staff, they may choose to provide the staff titles and individual hourly rates for that staff. It is assumed that the more complex jobs will take longer or be handled by different levels of staff.

2. Applicants must Provide the Total Cost for the estimated 1,500 Page total, using one of the provided base rates in the table above. The total number of pages needing remediation may be reduced or increased to meet the County's needs. **Only the Total Cost will be evaluated.**

3. Rates must be fully burdened: these rates must include all costs for benefits, profit, and overhead. Travel is not required, therefore travel time or mileage is not reimbursable under this contract.

ATTACHMENT B, MANDATORY INSURANCE REQUIREMENTS

Prior to the execution of the contract by the County, the proposed awardee/contractor must obtain, at their own cost and expense, the following *minimum* (not maximum) insurance coverage with an insurance company/companies licensed to conduct business in the State of Maryland and acceptable to the Division of Risk Management. This insurance must be kept in full force and effect during the term of this contract, including all extensions. The insurance must be evidenced by a certificate of insurance, and if requested by the County, the proposed awardee/contractor shall provide a copy of the insurance policies and additional insured endorsements. The minimum limits of coverage listed below shall not be construed as the maximum as required by contract or as a limitation of any potential liability on the part of the proposed awardee/contractor to the County nor shall failure to request evidence of this insurance in any way be construed as a waiver of proposed awardee / contractor's obligation to provide the insurance coverage specified. The Contractor's insurance shall be primary with the County's being non-contributory.

Commercial General Liability
A minimum limit of liability of five hundred thousand dollars ($500,000) per occurrence for bodily injury, personal injury and property damage coverage per occurrence, including the following coverages:

Contractual Liability
Premises and Operations
Independent Contractors & Subcontractors
Products and Completed Operations

Professional Liability (Errors and Omissions Liability)
The policy shall cover professional errors and omissions, negligent acts, misconduct or lack of ordinary skill during the period of contractual relationship and services rendered with the County with a limit of liability of at least:

Each Claim $1,000,000

In the event that the professional liability insurance required by this Contract is written on a claims-made basis, Contractor warrants that any retroactive date under the policy shall precede the effective date of this Contract; and that either continuous coverage will be maintained or an extended discovery period will be exercised for a period of three (3) years beginning at the time work under this Contract is completed.

Subcontractor Requirements
Unless otherwise stated below the proposed awardee/contractor shall require all subcontractors to obtain, and maintain, insurance with limits equal to, or greater, than those limits required within the contract.

Additional Insured
Montgomery County, Maryland, its elected and appointed officials, officers, consultants, agents and employees, must be included as an additional insured on an endorsement to Contractor's commercial general, and contractor's excess/umbrella insurance policies, if used to satisfy the Contractor's minimum insurance requirements under this contract, for liability arising out of contractor's products, goods and services provided under this contract. The stipulated limits of coverage above shall not be construed as a limitation of any potential liability of the contractor. Coverage pursuant to this Section shall not include any provision that would bar, restrict, or preclude coverage for claims by Montgomery County against Contractor, including but not limited to "cross-liability" or "insured vs insured" exclusion provisions.

Policy Cancellation
Should any of the above policies be canceled before the expiration date thereof, written notice must be delivered to the County in accordance with the policy provisions.

Certificate Holder
Montgomery County, Maryland
Department of Environmental Protection /DEP Contracts Team
2425 Reedie Drive. 4th Floor
Wheaton, MD 20902

All Certificates of Insurance must be sent to DEP.Procurments@montgomerycountymd.gov.
Hard copy COI's are not requested or required.

ATTACHMENT C,
REFERENCES

(must submit at least three)

You are requested to provide references to the County with your proposal. The three (3) references must be from individuals or firms for whom work of a similar scope has been performed within the last three years. Names for references shall be of individuals who directly supervised or had direct knowledge of the services or goods provided.

NAME OF FIRM: ______________________________

ADDRESS: ______________________________

CITY: ______________ STATE: __________ ZIP: __________

CONTACT PERSON: ______________ PHONE: __________

EMAIL: ______________ CELL PH __________

NAME OF FIRM: ______________________________

ADDRESS: ______________________________

CITY: ______________ STATE: __________ ZIP:

CONTACT PERSON: ______________ PHONE: __________

EMAIL: ______________ CELL PH __________

NAME OF FIRM: ______________________________

ADDRESS: ______________________________

CITY: ______________ STATE: __________ ZIP:

CONTACT PERSON: ______________ PHONE: __________

EMAIL: ______________ CELL PH __________

ATTACHMENT D, SAMPLE REMEDIATION DOCUMENTS

* All three documents must be remediated per the Scope of this RFP and submitted as part of the Contractors submission package to be evaluated. **Documents must be submitted as separate files.**

1. https://montgomerycountymd.gov/dep/Resources/Files/archive/sample1.pdf

2. https://montgomerycountymd.gov/dep/Resources/Files/archive/sample2.pdf

3. https://montgomerycountymd.gov/dep/Resources/Files/archive/sample3.pdf

ATTACHMENT E, SAMPLE CONTRACT

CONTRACT
BETWEEN MONTGOMERY COUNTY, MARYLAND
AND
CONTRACTOR NAME TBD
CONTRACT #1193001

PDF REMEDIATION FOR ACCESSIBILITY COMPLIANCE

This Contract is between Montgomery County, Maryland (the “County”) and CONTRACTOR NAME AND ADDRESS TBD (the “Contractor”). The County and Contractor together are the “Parties.”

1. BACKGROUND AND INTENT:

Montgomery County, Maryland, through its Department of Environmental Protection (“Department”), has a broad range of Portable Document Files (PDFs) used in support of the Department’s various initiatives.

The United States Department of Justice approved and published a rule updating Title II of the Americans with Disabilities Act (ADA) in the Federal Register requiring US state and local jurisdictions to meet Level AA of the Web Content Accessibility Guidelines (WCAG) Version 2.1. Montgomery County is required to comply with the updated regulation for Title II of the ADA by 4/24/2026.

The County requires services to remediate these PDFs to be fully compliant with the WCAG and to make all PDF content accessible to individuals with disabilities, including those using assistive technologies such as screen readers. To secure these services, the County issued informal Solicitation 1193001, PDF Remediation for Accessibility Compliance (“Solicitation”).

The Contractor submitted a response to the Solicitation (“Proposal”).

The County awards this Contract to the Contractor in accordance with the Solicitation.

The Contractor represents that it is willing and able to complete the services and provide the goods set forth in this Contract, the Solicitation, and its Proposal to the satisfaction of the County.

2. SCOPE OF WORK

A. The Contractor must provide the following services to the County in accordance with the requirements of the Solicitation:

1) Document Assessment

a) Review and assess all provided PDF documents.

b) Identify accessibility issues and remediation requirements.

c) Provide a report summarizing findings and estimated effort per document.

2) PDF Remediation

a) Apply proper tagging structure (headings, lists, tables, etc.)

b) Add alternative text for all meaningful images and graphics.

c) Ensure correct reading order and logical document structure.

d) Remediate tables for accessibility (headers, scope, summaries, etc.).

e) Ensure form fields are interactive and accessible (if applicable).

f) Remove or remediate inaccessible elements (e.g., scanned text without OCR).

g) Ensure color contrast and font readability.

h) Remediated documents must comply with WCAG 2.1 Level AA standards (Attachment F, Solicitation).

3) Quality Assurance

a) Conduct internal Quality Assurance (QA) using assistive technologies such as screen readers and accessibility checkers (e.g., Adobe Acrobat Pro, JAWS, NVDA, VoiceOver, PAC2024).

b) Validate compliance with WCAG 2.1 Level AA and Portable Document Format/Universal Accessibility (PDF/UA) Standards (Attachment F, Solicitation).

c) Provide a compliance report for each remediated document.

B. The Contractor must provide the following deliverables to the County in accordance with the requirements of the Solicitation:

1) Fully remediated and accessible PDF files;

2) Accessibility compliance reports for each document;

3) Bi-weekly summary report of all remediated documents and compliance status.

C. The Contractor must perform all work in strict conformity with the requirements of the Solicitation as fully set forth therein, and in accordance with the Contractor’s Proposal, both of which are incorporated into this Contract as Attachment A and Attachment B, respectively. The Department will provide final approval of all deliverables.

D. The Contractor must guarantee their work. If corrections are needed, the Contractor must remediate all errors at no extra cost to the County.

3. INFORMATION SECURITY

The Contractor must use commercially responsible efforts to ensure that the County’s information resources, including electronic data assets, are protected from theft, unauthorized destruction, use, modification, or disclosure as deemed necessary under the County’s Information Resources Security Procedure (Administrative Procedure 6-7). To the extent the Contractor has access to the County’s network, the Contractor must adhere to Administrative Procedure 6-7 (Attachment G, Solicitation).

4. CONTRACT ADMINISTRATION AND CONTACTS

A. Montgomery County

Authority. The Director, Office of Procurement, is the delegated contracting officer. Therefore, the Director, Office of Procurement, must approve amendments, modifications, or changes to the terms, conditions, or minority, female, and disabled subcontractor plans in writing.

1. Contract Administrator and Project Manager:

Contract Administrator - The County will designate a Contract Administrator to oversee the administration of this Contract, in accordance with paragraph 6 of the General Conditions of Contract Between County and Contractor. The Contract Administrator has the duties and responsibilities described in paragraph 6, Contract Administration, of the General Conditions of Contract Between County and Contractor. The Contract Administrator for this Contract is:

Scott Faunce

IT Operations and Infrastructure Management Supervisor

Under the Contract Administrator, the County will assign a Contract Manager who will coordinate issuing assignments and be the point of contact for assignments and work-related questions and concerns. The Contract Manager is:

Cat Lee

IT Specialist III

B. Contractor

Contract Administrator. The Contractor must designate a Contract Administrator to oversee the administration of this Contract. The Contract Administrator must monitor the Contractor's adherence to the terms and conditions of the Contract and be the point-of-contact for administering, managing, and facilitating all Contract-related issues and activities, as well as coordinate communications for all work assignments.

The Contractor's Contract Administrator must ensure compliance with all requirements of the Solicitation, including those in Section D.3, Contractor's Responsibility.

The Contractor's Contract Administrator is:

TBD: NAME, TITLE
CONTRACTOR
ADDRESS
PHONE
EMAIL

5. TERM

The effective date of this Contract begins upon signature of the Director, Office of Procurement, and ends after **one** year or until compensation under this Contract reaches $**99,999.00**, whichever comes first. Before this term ends, the Director at his/her sole option, may (but is not required to) renew the Contract, if the Director determines that renewal is in the best interest of the County. The Contractor's satisfactory performance does not guarantee renewal of this Contract. The Director may exercise this option to renew this term **two** times for four years each. Any contract renewals are contingent upon appropriation and encumbrance of funds.

6. COMPENSATION, INVOICES, AND PRICE ADJUSTMENT

A. Compensation: The County will make payment to the Contractor within thirty (30) calendar days following the County's receipt, acceptance, and approval of the Contractor's invoice.

Compensation will be based on the costs submitted as part of the Contractor's proposal. Any equipment purchased with County funds becomes the property of the County.

The County will not pay any mark-up or fees on Other Direct Costs (ODC), nor compensate for mileage, travel, per diem, or travel time.

Compensation for work issued on a task-order basis will be on an hourly rate or a per unit basis as specified in each Task Order Proposal Request (TOPR).

Total compensation under this Contract must not exceed $99,999.00 for the entire Contract term (initial term plus any renewal terms exercised by the County), and inclusive of any fees, expenses, or costs. If the Contractor receives a Task Order from the County that will result in total compensation exceeding $99,999.00, the Contractor must contact the County's Contract Administrator prior to any performance under the Task Order.

Compensation must not exceed funds appropriated by the County and encumbered into a County Purchase Order issued to the Contractor. No services will be performed or compensated under this Contract prior to the execution of a County Purchase Order and the Contractor's receipt of said County Purchase Order.

B. Invoices: The Contractor must submit written and signed invoices in a format approved by the County. The Contract Administrator or designee will advise the Contractor of any required supporting documentation that must be submitted with each invoice. Invoices must be emailed to DEP.Invoice@montgomerycountymd.gov.

- Each invoice must cover only work reviewed and accepted by the County and must include any required documentation.
- Invoices must be submitted using the rates provided in the Contractor's Proposal.
- Invoices in good format and approved by the County will be paid in accordance with the County procedures for prompt payment within 30 calendar days of receipt, acceptance, and approval of a true and correct invoice. Payment is subject to verification of work performed and upon the County's approval of written invoices. The County may request additional documentation for invoice charges.
- If the County objects to any portion of the Contractor's invoice, the County will notify the Contractor and, at the County's discretion, may either pay the approved portion of the invoice or reject the invoice in its entirety and return it to the Contractor for correction.

The following information, at a minimum, must be included on each invoice, dated and on company letterhead:

- Contract and Purchase Order Number(s)
- Unique, sequential Invoice number of at least four characters
- Name, telephone number, and e-mail of a contact person
- Signature of Contract Manager
- Tracking of purchase order balances of funds expended and funds remaining.

C. Price Adjustment

Prices are firm for a period of one year after execution of the contract. Any request for a price adjustment after this one-year period is subject to the following:

1) Approval or rejection by the Director, Office of Procurement or designee.
2) Must be submitted in writing to the Director, Office of Procurement, and accompanied by supporting documentation justifying the Contractor's request. A request for any price adjustment may not be approved unless the Contractor submits to the County sufficient justification to support that the Contractor's request is based on its net increase in costs in delivering the goods/services to the County under the contract terms.
3) Must be submitted sixty (60) days prior to the contract expiration date, if the contract is being amended.

4) May not be approved in an amount that exceeds the annual percentage change of the Consumer Price Index (CPI) for the twelve-month period immediately prior to the date of the request. The request must not exceed the CPI for all urban consumers issued for the Washington-Arlington-Alexandria, DC-VA-MD-WV Metropolitan area by the United States Department of Labor, Bureau of Labor Statistics for ALL ITEMS. The County will approve only one price adjustment for each contract term, if a price adjustment is approved.

5) Should be effective sixty (60) days from the date of receipt of the Contractor's request.

6) Must be executed by written contract amendment.

7. GENERAL CONDITIONS BETWEEN COUNTY AND CONTRACTOR, AND INSURANCE

The General Conditions of Contract Between County and Contractor ("General Conditions"), Section B of the Solicitation (Exhibit A), are incorporated herein and made a part of this Contract, except that the mandatory insurance requirements listed in Attachment B to the Solicitation supersede those listed in provision 21 of the General Conditions.

8. PRIORITY OF DOCUMENTS

The following documents are incorporated by reference into and made part of this Contract. In the event of a conflict among the documents comprising this Contract, the order of priority for the purposes of resolving conflicts is:

A. This Contract document;

B. The General Conditions of Contract Between County and Contractor (Section B, Solicitation) and Mandatory Insurance Requirements (Attachment B, Solicitation);

C. Informal Solicitation 1193001, inclusive of all attachments and any amendments (Exhibit A);

D. Proposal from Contractor, inclusive of its cost proposal (Exhibit B).

E. Montgomery County Administrative Procedure 6-7, Information Resources Security (Attachment C);

9. SIGNATURES

CONTRACTOR TBD

By: ______________________________

Typed: TBD

Title: TBD

Date: ______________________________

MONTGOMERY COUNTY, MARYLAND

By: ______________________________
Avinash G. Shetty, Director
Office of Procurement

Date: ______________________________

RECOMMENDED

By: ______________________________
Jeffrey Seltzer, Deputy Director
Department of Environmental Protection

Date: ______________________________

APPROVED AS TO FORM BY THE OFFICE OF THE COUNTY ATTORNEY

By: ______________________________
Tram-Anh (Annie) Tran
Assistant County Attorney

Date: ______________________________

ATTACHMENT F, REQUIRED DOCUMENT STANDARDS

1. WCAG 2.1 Level AA Standards - https://www.w3.org/TR/WCAG21/.

2. Portable Document Format/Universal Accessibility (PDF/UA) Standards - https://www.adobe.com/uk/acrobat/resources/document-files/pdf-types/pdf-ua.html.

ATTACHMENT G,
MONTGOMERY COUNTY ADMINISTRATIVE PROCEDURE 6-7, INFORMATION SECURITY

Cover Page

Attachment G

	MONTGOMERY COUNTY ADMINISTRATIVE PROCEDURE **Office of the County Executive • 101 Monroe Street • Rockville, Maryland 20850**	NO. 6-7 PAGE Page **1** of **5** DATE 07/26/2024
TITLE Information Security		CAO APPROVAL

1.0 PURPOSE & SCOPE

1.1 To establish an Administrative Procedure (AP) for the users of the County's Information Systems to ensure that the County's Information Systems are used and administered in a manner that protects it from unauthorized or inadvertent access, use, destruction, modification, disclosure, theft, or denial of service.

2.0 DEFINITIONS

2.1 Compliance–Mandated Departments or Information Systems – Departments or Information Systems that process, store, and/or transmit data subject to security restrictions imposed by the Federal and State governments, the Health Insurance Portability and Accountability Act (HIPAA), FBI Criminal Justice Information Services Division (FBI CJIS), and the Payment Card Industry Data Security Standard (PCI–DSS).

2.2 Department of Technology and Enterprise Solutions (TEBS) – An Executive Branch department responsible for County government enterprise information systems and telecommunications.

2.3 Office of Enterprise Information Security (OEIS) – An office within TEBS that is responsible for the security of the County's Information Systems.

2.4 Information System – A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

2.5 Information System Registry – A central repository containing information on Information Systems.

2.6 Users – Any appropriately provisioned individual with a requirement to access a County information system.

2.7 Using Department ("department") – a department or office that owns or uses an Information System.

3.0 POLICY

3.1 Montgomery County Government will implement security policies following security controls and associated assessment procedures defined in the most current revision of NIST SP 800–53 Recommended Security Controls for Federal Information Systems and Organizations, as adapted for County use.

3.2 Users must review and abide by the AP 6–7 Information Security Rules of Behavior Handbook. The handbook describes the rules associated with user's responsibilities in the use of an Information System.

3.3 All departments, system owners, and data owners must review and abide by the AP 6–7 Information Security System and Data Owners Handbook, and must develop, document, and disseminate to their department users procedures that implement this Administrative Procedure and associated handbooks.

3.4 Compliance–Mandated Departments, County Information System owners, and data owners must use this Administrative Procedure as baseline policy, and develop, document, and disseminate to their users Information System policies and procedures based on compliance specific guidelines. The policies and procedures must be managed by a designated official within the department.

3.5 TEBS must maintain and publish the Information Security Rules of Behavior Handbook and the Information Security System and Data Owners Handbook addressing the following NIST SP 800–53 Recommended Security Controls families:

- Information Access Control
- Information Security Awareness and Training
- Audit and Accountability
- Information Security Assessment, Authorization and Monitoring
- Configuration Management
- Contingency Planning
- Identification and Authentication
- Incident Response
- Maintenance
- Media Protection
- Physical and Environmental Protection
- Planning
- Personnel Security
- Risk Assessment
- System and Services Acquisition
- System and Communication Protection
- System and Information Integrity
- Program Management
- Exemption from Administrative Procedure

3.6 Exemptions – Any deviations from this policy, including the Information Security Rules of Behavior Handbook and the Information Security System and Data Owners Handbook, require an exemption request to be submitted in writing by the using department and approved in writing by TEBS OEIS. The request must describe a) the business case justification, b) compensating controls, c) duration, and d) the specific user, system, or application to be exempted. TEBS OEIS must track and report on exemptions granted.

3.7 Information System Registration – Using departments must register all Information Systems with TEBS and keep the registry updated at all times.

3.8 Information System Authorization – A risk assessment must be performed and approved by TEBS, before any new Information System is put in production. Periodic risk assessments must be performed for existing Information Systems, as determined by TEBS. Operations of any Information System not approved by TEBS must have an approved exemption or be removed from operations.

3.9 Violation of this Administrative Procedure is prohibited and may lead to disciplinary action, including dismissal, and other legal remedies available to the County. A County employee who violates this Administrative Procedure may be subject to disciplinary action, in accordance with Montgomery County law and executive regulations, including without limitation, the County’s Personnel and Ethics laws and regulations, currently codified in Chapters 33 and 19A of the County Code and COMCOR Chapters 33, and 19A, respectively, and applicable collective bargaining agreements, as amended.

3.10 In any contract where a contractor or business partner may have remote access to, or otherwise work or interface with, Information Systems, the following language, or language of similar import, must be included in the solicitation document and the contract, and AP 6–7 must be attached:

The Contractor may be afforded remote access privileges to County Information Systems, or otherwise work on or interface with County Information Systems, and must ensure that the County Information Systems, including electronic data assets, are protected from unauthorized or inadvertent access, use, destruction, modification, disclosure, theft, or denial of service. The Contractor must adhere to the County's Information Security Administrative Procedure (AP 6–7), which is attached to, incorporated by reference into, and made a part of this contract.

3.11 The County reserves the right to enforce training using progressive discipline procedures that may include performance evaluation and temporary Active Directory (AD) account lockout for a user’s failure to complete all County mandatory training.

4.0 RESPONSIBILITIES

4.1 User – User must use County Information System(s) for County business purposes only and in compliance with this Administrative Procedure.

4.2 Department

4.2.1 Ensures users participate in the County's Information Security Awareness Training Program and comply with the County's information technology security procedures including this Administrative Procedure and the Information Security Rules of Behavior Handbook and the Information Security System and Data Owners Handbook.

4.2.2 Enunciates department–specific information security policies and procedures and trains users on them.

4.2.3 Reviews and updates department–specific information security policies and procedures annually.

4.2.4 Incorporates this Administrative Procedure in any contract that requires a contractor's employees or its agents to have access to County Information Systems.

4.2.5 Cooperates with TEBS in the vulnerability testing and remediation process of department–operated Information Systems assets.

4.2.6 Reports security incidents per procedure and assists in their investigation and prevention.

4.2.7 Assists TEBS with maintaining County Information Systems in compliance with this Administrative Procedure.

4.2.8 Ensures that all Information Systems used for County business are registered with TEBS and updated annually.

4.2.9 Regularly update software to ensure that it is currently supported by the vendor and that applicable security patches are installed.

4.2.10 Reports on compliance with the policies stated in the Information Security Rules of Behavior Handbook and the Information Security System and Data Owners Handbook.

4.3 TEBS

4.3.1 Provides information security awareness training.

4.3.2 Reports information security risk and compliance status to the Chief Administrative Officer.

4.3.3 Advises departments on information security issues.

4.3.4 Assists departments in the remediation of identified vulnerabilities.

4.3.5 Advises departments in the secure design of County Information Systems.

4.3.6 Periodically conducts security scans and vulnerability testing to identify vulnerabilities.

4.3.7 Leads investigations and responses to County Information System security incidents.

4.3.8 Monitors County Information System security threats and manages countermeasures.

4.3.9 Reviews County Information System solicitations/contracts for inclusion of this Administrative Procedure.

4.3.10 Performs/evaluates risk assessments for all new Information Systems, and periodically for all existing County Information Systems identified as critical/sensitive by the using department and or TEBS.

4.3.11 Maintains and implements enterprise County Information System security measures and reviews and updates information security policies and handbooks.

4.3.12 Manages the exemption process.

4.3.13 Monitors and reports on data owners' and departments' compliance with this Administrative Procedure.

4.4 County

4.4.1 Determine and provide approved hardware and peripheral devices to users.

5.0 DEPARTMENTS AFFECTED

5.1 All Executive Branch departments and offices.

6.0 APENDICIES

6.1 Information Security Rules of Behavior Handbook.

6.2 Information Security System and Data Owners Handbook

INFORMATION SECURITY

RULES OF BEHAVIOR (ROB)

Contents

1. Introduction and Purpose

The Information Security Rules of Behavior Handbook describes the rules associated with user's responsibilities and certain expectations of behavior using County Information Systems and while connected to the County network, as required by Administrative Procedure 6–7. This handbook makes users aware of their role in safeguarding County Information Systems and applies to all County employees, volunteers, interns, contractors, and business partners always, regardless of how or where they access County Information Systems.

2. Information Security Rules of Behavior

2.1. General

2.1.1. All Information contained in, stored on, transmitted by, and/or received by County Information Systems is the sole property of the County, and as such, Users must have reasonable expectations that individuals approved by the County may, when appropriate, view, modify, and/or delete this information.

2.1.2. All activities performed on County Information Systems may be monitored or logged.

Users must:

2.1.3. Follow security practices that are the same as or equivalent to those required at their primary work location when working at any alternate work location.

2.1.4. Only use County-provided and approved infrastructure or cloud solutions for conducting County business and storing County Information.

2.1.5. Only use the County-provided email/calendaring/collaboration solution (Office 365) when performing County work.

2.1.6. Complete all County Mandatory Security Awareness Training prior to the close of business on the last day of the same month in which the training was initiated.

2.2. Accessing or Using County Information Systems

Users must:

2.2.1. Utilize Multi-Factor Authentication (MFA) provided by the County when accessing County Information Systems.

2.2.2. Only access County Information Systems and Information that is required in the performance of their official duties.

2.2.3. Promptly report to the IT Help Desk any observed or suspected security problems/incidents, including but not limited to:

2.2.3.1. Loss or theft of County Information Systems;

2.2.3.2. Persons requesting that a User disclose their password; or

2.2.3.3. Phishing attempts which include emails, messages, or other communications that appear to be fraudulent or malicious in nature and attempt to deceive Users into disclosing Sensitive Information.

2.2.4. Protect County Information Systems and Sensitive Information per departmental procedures and report any unauthorized access, copying, or use of County Information Systems and Sensitive Information that is not necessary to perform the User's County-assigned responsibilities.

2.2.5. Protect Information Systems from theft, destruction, or misuse at all times, including teleworking and when not in use.

2.2.6. Abide by copyright laws applicable to any licensed software.

2.2.7. Promptly change a password whenever it is compromised or suspected to be compromised.

2.2.8. Maintain the confidentiality of passwords and are responsible for actions performed with their accounts.

2.2.9. Report unauthorized personnel that appear in the work area to a department-designated individual, immediate supervisor, or the Security Services Division who must then report the incident to the OEIS via a Help Desk ticket.

2.2.10. Protect County Sensitive Information stored on electronic media or in any physical format, such as paper.

2.2.11. Encrypt Sensitive Information contained within the body of an email or contained within the attachment to an email using County-approved encryption software.

2.2.12. Encrypt Portable Storage Devices when there is a business need to store Sensitive Information with AES-256-bit encryption based on the sensitivity level.

2.2.13. Lock County Information Systems with a password when away from the work area (on-site and off-site), including for meals, breaks, or any extended period.

2.2.14. Ensure that all Sensitive Information in hard copy or electronic form is secured when not in use, including at the end of the day and when they are expected to be gone for an extended period.

2.2.15. Delete, reformat, or shred sensitive information when no longer needed in accordance with County/Departmental policies and procedures, applicable laws, and regulations, including without limitation applicable State archival laws and Administrative Procedure 6-3.

2.2.16. Keep file cabinets containing Sensitive Information closed and locked when not in use or when not attended.

2.2.17. Remove printouts containing Sensitive Information immediately from the printer or fax and adhere to secure printing practices by utilizing the printer's "Log-In-To-Print" functionality when made available.

2.2.18. Shred documents containing Sensitive Information immediately upon disposal, or place the documents in official shredder bins, or locked confidential disposal bins **only if** consistent with applicable law, Administrative Procedure 6-3, and any litigation holds,

2.2.19. Erase whiteboards containing Sensitive Information when leaving the work area unattended.

2.2.20. Lock away portable computing devices such as laptops and tablets.

Users must NOT:

2.2.21. Write, display, or store passwords where others may access or view them, such as but not limited to leaving passwords written on sticky notes posted on or under a computer.

2.2.22. Leave keys used for access to Sensitive Information at an unattended desk.

2.2.23. Download software or code from the Internet while connected to the County's network, unless explicitly approved and authorized by the County, as such downloads may introduce malware to the County's network.

2.2.24. Obtain, install, replicate, or use unlicensed software unless authorized by their Department.

2.2.25. Open emails from suspicious sources.

2.2.26. Use peer-to-peer networking unless approved by the County or required for vendor support. Users must not conduct software or music piracy, hacking activities, or participate in online gaming.

2.2.27. Acquire, possess, or use hardware or software tools to bypass software copy protection, discover passwords, identify security vulnerabilities, or circumvent encryption.

2.2.28. Attempt unauthorized access to an Information System, including attempting to access the Information contained within the system.

2.2.29. Use copyrighted or otherwise legally protected material without permission.

2.2.30. Transmit chain letters, unauthorized mass mailings, or intentionally send malware.

2.2.31. Use any personal computers/devices for County business or County Information System that show signs of being infected by a virus or other malware.

2.2.32. Alter hardware or software settings on any County Information Systems without permission.

2.2.33. Authorize or make a ransom payment.

2.2.34. Add any devices to the County network without permission from TEBS.

2.2.35. Create automated forwarding rules or mechanisms within their County email accounts that automatically forward County emails to any address outside of the County’s network, including personal email accounts.

2.3. International Travel (for work or non-work travel)

2.3.1. Pre-Travel Preparation

Users must:

2.3.1.1. Review the U.S. Department of State Travel Advisories website (https://travel.state.gov/content/travel/en/traveladvisories/traveladvisories.html/) to determine if the use of County-owned devices or the access to County systems is permissible. Accessing County systems or bringing County-owned devices while on travel to or through countries with a Level 3 (Reconsider Travel) or Level 4 (Do Not Travel) advisory is strictly prohibited.

2.3.1.2. Obtain loaner Computing Device(s) (laptop, tablet, smartphone) from the County when traveling outside of the United States when intending to access County systems unless traveling to or through a country where bringing a County-owned device is prohibited as covered in 2.3.1.1.

2.3.1.3. Notify the Office of Enterprise Information Security (OEIS) in advance (HelpIT@montgomerycountymd.gov) when traveling to a foreign country with a County-owned device or will access County systems providing the following Information:

- Travel dates;
- Nature of business;
- Itinerary; and
- Device(s) name/number.

2.3.1.4. Notify OEIS immediately should travel dates, nature of business, itinerary, and/or device(s) names/numbers be modified.

2.3.1.5. Backup their County data in a County-approved County Information System.

2.3.1.6. Become aware of known political unrest, natural disasters, economic concerns, and/or criminal activities or the potential thereof occurring in destinations identified in the User's itinerary.

2.3.1.7. Ensure the following (where and when appropriate) when utilizing a loaner device on international travel:

- Verify with the individual issuing the loaner device that the latest software patches have been installed;
- Verify with the individual issuing the loaner device that County approved encryption software has been installed (based on individual County laws/regulations);
- Verify with the individual issuing the loaner device that the latest versions of County approved security software have been installed;
- Verify with the individual issuing the loaner device that the County's VPN (Virtual Private Network) has been installed;
- No County Information has been stored on the device; and
- Proper locking devices have been obtained.

2.3.1.8. Send emails with your questions about securing data on your trip to HelpIt@montgomerycountymd.gov

2.3.2. While Traveling

Users must:

2.3.2.1. Notify OEIS immediately of any modification to travel dates, nature of business, itinerary, and/or device(s) names/numbers.

2.3.2.2. Utilize the County's VPN when connecting to County Information Systems.

2.3.2.3. Report suspicious activity immediately to the County's Helpdesk immediately upon detection.

2.3.2.4. Only connect to trusted wi-fi networks.

2.3.2.5. Connect only to HTTPS websites as need dictates.

2.3.2.6. Turn off wi-fi immediately after use.

2.3.2.7. Utilize County-provided locking devices appropriately.

2.3.2.8. Always maintain physical control of all County devices.

Users must not:

2.3.2.9. Use County assigned administrator accounts.

2.3.2.10. Plug in any accessories provided by anyone other than known County personnel.

2.3.2.11. Enter County credentials into public devices.

2.3.2.12. Share or allow others to take control of County devices other than known County personnel.

2.3.2.13. Store any Information on County devices.

2.3.3. Return to Office

Users must:

2.3.3.1. Notify OEIS of your return home by emailing HelpIt@montgomerycountymd.gov.

2.3.3.2. Clear internet browsing history for the length of time that travel occurred.

2.3.3.3. Change County passwords that were utilized during travel.

2.3.3.4. Return all loaner devices.

TEBS/Department must:

2.3.3.5. Clean all loaner devices upon return.

OEIS must:

2.3.3.6. Run appropriate scans.

3. Appendices

3.1. Definitions

TERM:	DESCRIPTION:
Compliance–Mandated Departments or Information Systems	Departments or Information Systems that process, store, and/or transmit data subject to security restrictions imposed by the Federal and State governments, the Health Insurance Portability and Accountability Act (HIPAA), the FBI Criminal Justice Information Services Division (FBI CJIS), and the Payment Card Industry Data Security Standard (PCI–DSS).
Computing Device	Any electronic equipment controlled by a CPU, including desktop and laptop computers, smartphones, and tablets.
Information	Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual.
Information System	A discrete set of Information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of Information.
Multi-Factor Authentication (MFA)	Authentication using two or more factors to achieve authentication. Factors include: (i) something you know (e.g. password/personal identification number (PIN)); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric).
Portable Storage Devices	A system component that can communicate with and be added to or removed from a system or network and that is limited to data storage—including text, video, audio, or image data—as its primary function (e.g., optical discs, external or removable hard drives, external or removable solid-state disk drives, magnetic or optical tapes, flash memory devices, flash memory cards, and other external or removable disks).
Sensitive Information	Any Information that by law or County policy cannot be publicly disclosed, including without limitation: A. Non–Public criminal justice Information; B. Credit or debit card numbers; C. An individual's first name or first initial and last name, name suffixes, or unique biometric or genetic print or image, in combination with one or more of the following data elements; a) A Social Security number; b) A driver's license number, state identification card number, or other individual identification number issued by a State or local government; c) Passport number or other identification number issued by the United States government;

	d) An Individual Taxpayer Identification Number; e) A financial or other account number that in combination with any required security code, access code, or password, would permit access to an individual's account; f) Medical records; or g) Health insurance Information.
User	Any appropriately provisioned individual with a requirement to access a County information system.

Information Security System and Data Owners Handbook (ISSADOH)

1 Contents

1. Introduction

1.1. Introduction/Purpose

This Information Security System and Data Owners Handbook has been developed as a support document to the County's Administrative Procedure (AP) 6-7. Its purpose is to define a set of Security Controls and Privacy Controls that provide a means for the County and its individual Information System Owners to manage risks while at the same time complying with Information Systems security and privacy policies and practices. The Security and Privacy Controls are intended to create a foundation for the development of Assessment methods and procedures that will be used to determine the effectiveness of the controls. Additionally, it is intended to improve communication among the County's Information System Owners by providing a common language and understanding of security, privacy, and risk management concepts. The controls contained within this Handbook are adapted from specific control families defined within NIST Special Publication (SP) 800-53. Although originally developed for Federal Information Resources the controls are considered guidelines and are intended to be flexible enough to apply to the information resources of both public and private sector organizations.

TEBS developed this handbook as a support document for AP 6-7, Policy 3.5 that states:

TEBS must maintain and publish the "Information Security Rules of Behavior Handbook" and the "Information Security System and Data Owners Handbook," which address the following NIST SP 800-53 Recommended Security Controls families.

2.1 Information Access Control
2.2 Information Security Awareness and Training
2.3 Audit and Accountability
2.4 Information Security Assessment, Authorization, and Monitoring
2.5 Configuration Management
2.6 Contingency Planning
2.7 Identification and Authentication
2.8 Incident Response
2.9 Maintenance
2.10 Media Protection
2.11 Physical and Environmental Protection
2.12 Planning
2.13 Program Management
2.14 Personnel Security
2.15 Information System Risk Assessment
2.16 Information System and Services Acquisition
2.17 Information System and Communication Protection
2.18 Information System and Information Integrity
2.19 Supply Management
2.20 Exemption from Administrative Procedure

1.2. Scope

The Montgomery County Information Security System and Data Owners Handbook (ISSaDOH Handbook) policies apply to all individuals that have been granted access to any County Information Technology System, including, but not limited to Montgomery County staff, volunteers, students, contractors, vendors, and Third Parties. These policies are deemed to always be in effect and, as such, apply whether an Information System User is working internally or at an external location (e.g., individual's location, home, office, etc.) on Montgomery County business. Further, they apply equally to all Information Systems that are owned/operated by Montgomery County. In cases where it is not practical for Third-Party service providers to be knowledgeable of and follow the specific requirements of this policy, Third-Party contracts must include adequate language and safeguards to ensure County information and Information Systems are protected at a level that is equal to or greater than that required by this policy. These Policies supersede any conflicting statement or statements in any prior policy document.

2. The Controls

2.1. Information System - Access Control – AC

2.1.1. User Account Management – AC-2

Information System Owners must:

2..1.1.1. Define and document the types of User accounts allowed for use within the Information System in support of departmental missions and business functions;

2..1.1.2. Assign account managers for all User or Service Accounts;

2..1.1.3. Establish conditions for group and role membership;

2..1.1.4. Specify authorized Users of the Information System, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;

2..1.1.5. Require documented approvals by Information System account managers for requests to create User accounts;

2..1.1.6. Create, enable, modify, disable, and remove User accounts;

2..1.1.7. Monitor the use of User accounts;

2..1.1.8. Disable User accounts when there has been no activity for a period of ninety(90) days;

2..1.1.9. Notify Information System account managers within seven (7) days;

1. When User accounts are no longer required;
2. When Users are terminated or transferred; and
3. When individual Information System usage or need-to-know changes for an individual;

2..1.1.10. Authorize access to the Information Systems based on:

1. Approved authorization from Information System Owner;
2. Intended Information System usage; and
3. Other attributes as required by TEBS or associated missions and business functions

2..1.1.11. Review User and Information System accounts for compliance with account management requirements at least annually;

2..1.1.12. Establish a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group; and

2..1.1.13. Align User and Service Account management processes with personnel termination and transfer processes.

2.1.2. Access Enforcement – AC-3

Information System Owners must:

2..1.2.1. Enforce approved authorization for Logical Access to Information Systems.

2.1.3. Least Privilege – AC-6

Information System Owners must:

2.1.3.1. Ensure that access to Information Systems is secure, by taking measures that include the following:

1. Employ the principle of Least Privilege within the environment, allowing only Authorized Access for Users (or automated Information System processes acting on behalf of Users) that are necessary to accomplish assigned tasks in accordance with County missions and business functions.
2. Reviews of the privileged accounts must be performed annually to validate the need for such privileges.
3. Privileges must be removed or reassigned, if necessary, to correctly reflect the County mission and business needs
4. Assign staff to perform an audit of privileged Information System account functions.

2.1.4. Unsuccessful Logon Attempts – AC-7

Information System Owners must:

2.1.4.1. Enforce a limit of three (3) consecutive invalid logon attempts by a User during a fifteen (15) minute time period; and

2.1.4.2. When the maximum number of unsuccessful attempts is exceeded, automatically lock the account/node for thirty (30) minutes or until released by an administrator.

2.1.5. Information System Use Notification– AC-8

The County must:

2.1.5.1 Display a warning banner to Users before granting access to the Information System that provides privacy and security notices consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidelines and state that:

1. Users are accessing a Montgomery County Government Information System;
2. Information System usage may be monitored, recorded, and subject to audit;
3. Unauthorized use of the Information System is prohibited and subject to criminal and civil penalties; and
4. Use of the Information System indicates consent to monitoring and recording.

Information System Owners must:

2.1.5.2 Configure the Information System so that the notification message or banner is retained on the screen until Users acknowledge the usage conditions and take explicit actions to log on to or further access the Information System; and

2.1.5.3 For publicly accessible Information Systems, configure the Computer Information Resource to

1. Display Information System use information conditions, before granting further access to the publicly accessible Information System;
2. Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such Information Systems that generally prohibit those activities; and

3. Include a description of the authorized uses of the Information System

2.1.6. Permitted Actions Without Identification or Authentication AC-14

Information System Owners must:

2.1.6.1 Identify User actions that can be performed on the Information System without some form of Username or password (for example, individuals accessing public websites or other publicly accessible federal Information Systems, individuals using personal mobile phones to receive calls, or receiving facsimiles).

2.1.6.2 Document with supporting rationale the User actions that can be performed without a form of a Username or password.

2.1.7. Remote Access AC-17

TEBS must:

2.1.7.1 Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of Remote Access allowed to an Information System.

Users and/or Departments must:

2.1.7.2 Not store County Sensitive Information on non-County controlled resources unless all Department and TEBS procedures in this handbook, all federal, state, County laws and policies are followed.

2.1.8.Wireless Access AC-18

TEBS must:

2.1.8.1 Must establish and document usage restrictions, configuration/connection requirements, and implementation guidance for Wireless Access to a County Information System. Wireless Access to a County Information System must be authorized by an Information Steward prior to allowing the connections.

2.1.9. Access Control for Mobile Devices AC-19

The County:

2.1.9.1 Must establish usage restrictions, configuration, connection requirements, and implementation guidance of County-controlled mobile devices by a User when outside of County offices.

2.1.9.2 Is not responsible for maintenance, damage, or loss of personally owned computers, data, or peripherals used by employees in the workplace.

Departments:

2.1.9.3 Sensitive Information must not be stored on non-County-controlled resources unless the Department ensures adherence to AP 6-7, all state and County laws and policies.

Users:

2.1.9.4 With access to County Information System on a County-owned mobile devices must lock the screen until the correct password is entered. When the mobile device is not in use, the User must store the device in a secure area and delete Sensitive Information when it is no longer needed. The Department is responsible for ensuring that Sensitive Information has been deleted from County-controlled mobile devices and determining the frequency of review.

2.1.10. Use of External Information Systems AC-20

TEBS must:

2.1.10.1 Establish terms and conditions for authorized individuals accessing County Information Systems from External or Third-Party Information Systems.

2.1.11. Publicly Accessible Content AC-22

The County and Information System Owners must:

2.1.11.1 Must designate and train authorized individuals to post information on publicly accessible information sites in accordance with AP 6-8 Social Media. The proposed content must be reviewed by designated personnel prior to posting to ensure non-public information is not included, and must remove such information if discovered.

2.1.12. Sensitive Information Access (COUNTY ADDED)

Users must:

2.1.12.1 Not access, copy, or use County Sensitive Information that is not necessary to perform the User's County-assigned responsibilities.

2.1.13. Device Lock (AC-11 County Added – Not in NIST LOW)

Users:

2.1.13.1 To protect Sensitive Information, a User must not leave the PC terminal area while Sensitive Information is displayed on the screen. An employee must never leave Sensitive Information on the computer terminal unattended. If necessary, the Information System Owner must ensure that a screen-locking feature is installed on the PC that blanks the screen until the correct password is entered.

2.2. Security Awareness and Training – AT

2.2.1. Information Security Awareness Training – AT-2

The County must:

2.2.1.1 Provide basic information security and privacy awareness training to Information System Users as part of initial training for new Users;

2.2.1.2 Train when required by Information System changes; and

2.2.1.3 Train regularly to include recognizing and reporting potential indicators of insider threat and User's Rules of Behavior.

2.2.2. Role Based Training – AT-3

Information System Owners must:

2.2.2.1 Ensure that role-based Information Security awareness training is provided to personnel with assigned security roles and responsibilities (personnel role example types include Information System administrators, Information System security personnel, and Information System privacy personnel):

1. Before authorizing access to the Information System or performing assigned duties;
2. When required by Information System changes; and
3. On a regularly scheduled basis.

2.2.3.– AT-4 Information Security Training Records AT-4 (NIST says 'and privacy & role-based')

The County must:

2.2.3.1 Document and monitor basic Information Security awareness training activities.

Information System Owners must:

2.2.3.2 Ensure that Information Security awareness training activities are documented and monitored; and

2.2.3.3 That individual training records are retained for at least six (6) years.

2.3. Audit and Accountability – AU

2.3.1. Audit Events – AU-2

Information System Owners must:

2.3.1.1 Verify that the auditable Components of Information Systems can Audit Event types for their specific departmental needs. (Examples of auditable event types are: successful and unsuccessful User Account logon events, Account management events, policy change, Information System events, all administrator activity, data deletions, data access, data changes, and permission changes.)

2.3.1.2 Coordinate the security audit function with OEIS and other County entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable event types;

2.3.1.3 Provide a rationale for why the auditable event types are deemed to be adequate to support after-the-fact investigations of security and privacy incidents; and

2.3.1.4 Audit and document the subset auditable events determined from Audit Event - (2.3.1.1) monthly.

2.3.2. Content of Audit Records – AU-3

Information System Owners must:

2.3.2.1 Ensure that Audit Records are generated in an Audit Trail containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.

2.3.3.Audit Storage Capacity – AU-4

Information System Owners must:

2.3.3.1 Allocate Audit Record storage capacity to accommodate the Audit Record retention requirements.

2.3.4. Response to Audit Processing Failures – AU-5

Information System Owners must:

2.3.4.1 Alert designated personnel, identified by Department heads, in the event of an audit processing failure within one (1) hour; and

2.3.4.2 Take the following additional actions: overwrite the oldest Audit Record if space is an issue.

2.3.5. Audit Review, Analysis, and Reporting – AU-6

Information System Owners must:

2.3.5.1 Review and analyze Information System Audit Records at least weekly for indications of inappropriate or unusual activity;

2.3.5.2 Report findings to designated personnel; and

2.3.5.3 Adjust the level of audit review, analysis, and reporting within the Information System when there is a change in Risk based on law enforcement information, intelligence information, or other credible sources of information.

2.3.6. Time Stamps– AU-8

Information System Owners must:

2.3.6.1 Use internal Information System clocks to generate time stamps for Audit Records; and

2.3.6.2 Record time stamps for Audit Records that can be mapped to Coordinated Universal Time or Greenwich Mean Time and meets one (1) second granularity of time measurement.

2.3.7. Protection of Audit Information– AU-9

Information System Owners must:

2.3.7.1 Protect audit information and audit tools from unauthorized access, modification, and deletion.

2.3.8. Audit Record Retention– AU-11

Information System Owners must

2.3.8.1 Retain Audit Records for at least one hundred eighty (180) days to provide support for after-the-fact investigations of security and privacy incidents and to meet regulatory and organizational information retention requirements.

2.3.9. Audit Generation– AU-12

Information System Owners must:

2.3.9.1 Provide Audit Record generation capability for the auditable event types in Audit Event - (2.3.1.1) at all Information System Components where audit capability is deployed/available.

2.3.9.2 Allow designated personnel, identified by Department heads, to select which auditable event types are to be audited.

2.3.9.3 Generate Audit Records for the event types defined in Audit Event - (2.3.1.1) with the information in the Content of the Audit Record.

2.4. Information Security Assessments and Privacy Assessments, Authorization, and Monitoring – CA

2.4.1. Security Controls Assessments and Privacy Controls Assessments – CA-2

TEBS must:

2.4.1.1 Develop a Security Controls Assessment Plan and Privacy Controls Assessment Plan that describes the scope of the Assessments including:

1. Security controls and privacy controls under Assessment;
2. Assessment procedures used to determine control effectiveness;
3. Assessment environment and Assessment team;

2.4.1.2 Ensure the Security Controls Assessment Plan and Privacy Controls Assessment Plan are reviewed and approved by the designated OEIS County representative prior to retaining an independent Assessor to conduct the Assessments.

2.4.1.3 Have an independent Assessor assess the security and privacy controls in the Information System pursuant to the Security Controls Assessment Plan, Privacy Controls Assessment Plan, and its environment of operation at least every four (4) years to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements.

2.4.1.4 Have an independent Assessor produce a Security Controls Assessment Report and a Privacy Controls Assessment Report that documents the results of the Assessments. The County should explicitly include in the contract with the independent Assessor the requirement for them to produce the Assessment report based on the Assessment Plans.

2.4.1.5 The independent Assessor should provide TEBS with Assessment Reports that document the type of Assessments performed and the results from each area assessed.

2.4.1.6 Include as part of Security Controls Assessments and Privacy Controls Assessments, an in-depth monitoring; Vulnerability scanning; malicious User testing; insider threat Assessment; performance and load testing of Departments' Computer Information Systems every three (3) years.

2.4.2. Information System Interconnections – CA-3

The County must:

2.4.2.1 Authorize connections from Information Systems to other non-County Information Systems using Interconnection Security Agreements;

2.4.2.2 Document, for each interconnection, the interface characteristics, security and privacy requirements, and the nature of the information communicated; and

2.4.2.3 Review and update Interconnection Security Agreements at least every two years or upon contract renewal.

2.4.3. Plan of Action and Milestones (POAMS) – CA-5

TEBS must:

2.4.3.1 Develop a Plan of Action and Milestones, called a Risk Registry for Information Systems, to document the planned remedial actions of the County to correct weaknesses or deficiencies noted during the Assessment performed in 2.15.2 and 2.15.3, or otherwise identified, to reduce or eliminate known vulnerabilities in Information Systems;

2.4.3.2 Update Risk Registry/Plan of Action and Milestones at least annually based on findings from the ISP Assessment Report, Security Controls Assessments, Privacy Controls Assessments, Risk Assessments, or Information System monitoring activities.

2.4.4. Information System Authorizations – CA-6

Information System Owners must:

2.4.4.1 Prior to purchase decisions, contract executions, and/or internal system implementation, must request that a Risk Assessment be performed by TEBS. Based on the results of the Risk Assessment, TEBS may or may not provide their written approval to proceed.

2.4.4.2 Periodic Risk Assessments must be performed for existing Information Systems that process, store, or transmit County information. Based on the results of the Risk Assessment, Information Systems not approved by TEBS are prohibited.

2.4.5. Continuous Monitoring/Risk Monitoring – CA-7

TEBS must

2.4.5.1 Ensure continuous Risk Monitoring is an integral part of the governance process that includes the following:

1. Effectiveness Monitoring
2. Compliance Monitoring
3. Change Monitoring

2.4.6. Penetration Testing CA-8 (County Added – Not in NIST Low)

TEBS must:

2.4.6.1 Perform Penetration Testing every three (3) years on Information Systems with High Risks.

2.4.7. Internal Information System Connections – CA-9

The County must:

2.4.7.1 Authorize internal connections of Information System Components to the Information System; and

2.4.7.2 Document, for each internal connection, the interface characteristics, security and privacy requirements, and the nature of the information communicated.

2.4.8. Information System Registration – (County Added)

Using Departments must:

2.4.8.1 As defined in AP 6-7 "Information Resources Security" Section 3.7 "County Information System Registration" – "Using Departments must register all Information Systems with TEBS and keep the registry updated at all times." Registration information must be updated at least annually or after a significant change occurs that impacts the registration.

2.5. Configuration Management – CM

2.5.1. Baseline Configuration – CM-2

Information System Owners must:

2.5.1.1 Develop, document, and maintain a current Baseline Configuration for their Information Systems; and

2.5.1.2 Review and update the Baseline Configuration of the Information Systems at least annually, when required due to significant change, and when Information System Components are installed or upgraded.

2.5.2. Configuration Change Control – CM-3

TEBS must:

2.5.2.1 Determine the types of changes to the Information System that are configuration-controlled;

2.5.2.2 Perform a Security Impact Analysis on proposed configuration-controlled changes submitted by Information System Owners.

2.5.2.3 Monitor and review Information System activities associated with configuration-controlled changes that pose a High Risk for the County.

Information System Owners must:

2.5.2.4 Ensure that only Department-approved configuration-controlled changes to the Information Systems are implemented.

2.5.2.5 Ensure that records of configuration-controlled changes to the Information Systems are documented and retained.

2.5.2.6 Report all significant configuration-controlled changes to the Information System to TEBS prior to implementation.

2.5.3. Security Impact Analysis and Privacy Impact Analysis – CM-4

TEBS must:

2.5.3.1 Identify and analyze changes to the Information Systems to determine potential security and privacy impacts prior to change implementation.

2.5.3.2 Notify the Information System Owners in the event that the requested change poses a significant security or privacy risk to the County.

Information System Owners must:

2.5.3.3 Analyze the risk determination provided by TEBS to decide whether to continue with the implementation or select an alternative implementation.

2.5.4. Access Restrictions for Change – CM-5

Information System Owners must:

2.5.4.1 Define, document, approve, and enforce physical and Logical Access restrictions associated with configuration-controlled changes to the Information Systems.

2.5.5. Configuration Settings – CM-6

Information System Owners must:

2.5.5.1 Establish and document Configuration Settings for Components within the County Information System using industry acceptable standards (e.g. CIS Benchmarks) that reflect the most restrictive mode consistent with operational requirements;

2.5.5.2 Implement the Configuration Settings;

2.5.5.3 Identify, document, and approve any deviations from established Configuration Settings for Information System Components based on operational requirements; and

2.5.5.4 Monitor and control changes to the Configuration Settings in accordance with County policies and procedures.

2.5.6. Least Functionality – CM-7

Information System Owners must:

2.5.6.1 Configure the Information Systems to provide only essential capabilities; and

2.5.6.2 Prohibit or restrict the use of functions, Ports, Protocols, and/or services defined by Information System Owners as not required for Information System operation. Information System Owners should create their own Configuration Baseline and include a justification statement as to how they determined the Configuration Baseline settings.

2.5.7. Information System Component Inventory – CM-8

Information System Owners must:

2.5.7.1 Develop and document an inventory of Information System Components that:

1. Accurately reflects the current Information System;
2. Includes all Components within the Information System boundary;
3. Is at the level of granularity deemed necessary for Information System Owners to track and report on a regular basis; and
4. Includes information deemed necessary for TEBS to achieve effective Information System Component accountability; and

2.5.7.2 Review and update the Information System Component inventory on a regularly scheduled basis or as changes occur.

2.5.8. Software Usage Restrictions – CM-10

TEBS, Departments, and Users must:

2.5.8.1 Use any licensed software and associated documentation in accordance with all applicable contractual terms, including, without limitation, any software license agreements.

TEBS and Departments must:

2.5.8.2 To the extent a contract or software license agreement tracks use by quantity of Users or other numeric value, track the use of the software and associated documentation to ensure it is consistent with the terms of the applicable contract or software license agreement to control copying and distributions.

Information System Owners must:

2.5.8.3 Control and document the use of Peer-to-Peer File Sharing Technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

2.5.9. User-Installed Software – CM-11

TEBS must:

2.5.9.1 Establish policies governing the installation of software by Users;

2.5.9.2 Enforce software installation policies; and

2.5.9.3 Monitor policy compliance continuously.

2.6. Contingency Planning – CP

2.6.1. Contingency Plan – CP-2

Information System Owners must:

2.6.1.1 Develop an Information System-specific Contingency Plan that:

1. Identifies essential missions and business functions and associated contingency requirements;
2. Provides recovery objectives and restoration priorities;
3. Addresses contingency roles, responsibilities, and assigned individuals with contact information;
4. Addresses maintaining essential mission and business functions despite an Information System disruption, compromise, or failure;
5. Addresses eventual, full Information System restoration (if applicable, based on Information System criticality) without deterioration of the security and privacy controls originally planned and implemented; and
6. Is reviewed and approved by OEMHS.

2.6.1.2 Distribute copies of the Contingency Plan to key contingency personnel;

2.6.1.3 Coordinate Contingency Planning activities with incident handling activities and the Office of Emergency Management and Homeland Security (OEMHS);

2.6.1.4 Review the Contingency Plan for the Information System at least annually;

2.6.1.5 Update the Contingency Plan to address changes to the County, Information Systems, or environment of operation and problems encountered during Contingency Plan implementation, execution, or testing;

2.6.1.6 Communicate Contingency Plan changes to key contingency personnel; and

2.6.1.7 Protect the Contingency Plan from unauthorized disclosure and modification.

2.6.2. Contingency Training – CP-3

Information System Owners must:

2.6.2.1 Provide Contingency Plan training to Information System Users consistent with departmental Contingency roles and responsibilities.

2.6.2.2 Perform training procedures using written and functional exercises, as appropriate, to determine the effectiveness of the plan and the County's readiness to execute the plan.

1. Train within thirty (30) days of assuming a contingency role and responsibilities;
2. Train when required by Information System changes; and
3. At least every four (4) years, thereafter

2.6.2.3 Be familiar with the Contingency Plan and its associated activation, recovery, and reconstitution procedures.

2.6.3. Contingency Plan Testing – CP-4

Information System Owners must:

2.6.3.1 Test the Contingency Plan for Information Systems that process, store, or transmit County Information at least every two years using practice simulated tests to determine the effectiveness of the plan and the County's readiness to execute the plan;

2.6.3.2 Review the Contingency Plan Test Results; and

2.6.3.3 Initiate corrective actions, if needed.

2.6.4. Alternate Storage Site – CP-6

TEBS, the Department of Police Security Services, and the Department of General Services must:

2.6.4.1 Establish an Alternate Storage Site including necessary agreements to permit the storage and retrieval of Information System Backup information for critical network Information Systems, if possible,

2.6.4.2 Ensure that the Alternate Storage Site provides security controls equivalent to that of the primary site.

2.6.4.3 Identify an Alternate Storage Site that is separated from the primary storage site to reduce susceptibility to the same threats.

Information System Owners must:

2.6.4.4 Backup data and files vital to the County's operations, mission, or security, as scheduled, and retain at least the last three (3) Backup copies. The backing up of data is to be commensurate with the frequency of change of the data and the importance of recovering the lost data in a timely manner.

2.6.4.5 Maintain Backups at a physically separate, environmentally controlled facility.

2.6.4.6 Identify potential accessibility problems to the Alternate Storage Site in the event of an area-wide disruption or disaster and outline explicit Mitigation actions.

2.6.4.7 Notify TEBS as soon as changes in facilities are determined.

2.6.5. Alternate Processing Site CP-7 (County Added – Not In NIST LOW)

TEBS, the Department of Police Security Services, and the Department of General Services must:

2.6.5.1 Establish an alternate processing site for the safety of Information Systems and personnel;

2.6.5.2 Identify an alternate processing site that is separated from the primary processing site to reduce susceptibility to the same threats;

2.6.5.3 Make available at the alternate processing site, the equipment and supplies required to transfer and resume operations or put contracts in place to support delivery to the site within the departmentally defined time-period for transfer and resumption; and

2.6.5.4 Provide information security and privacy safeguards at the alternate processing site that are equivalent to those at the primary site.

2.6.6. Information System Backup CP-9

Information System Owners must:

2.6.6.1 Conduct the following back-ups at a frequency that reflects the criticality of the system:

1. Incremental Backups and Full Backups of User-Level Information contained in the Information System;

2. Incremental Backups and Full Backups of Information System-Level Information contained in the Information System;

3. Incremental Backups and Full Backups of Information System documentation including security-related documentation; and

2.6.6.2 Protect the confidentiality, integrity, and availability of Backup information at storage locations.

2.6.7. Information System Recovery CP-10

Information System Owners must:

2.6.7.1 Provide for the recovery and reconstitution of the Information System to a known state after a disruption, compromise, or failure.

2.6.7.2 Focus on implementing recovery strategies during recovery activities to restore Information System capabilities through the restoration of Information System Components, repair of damage, and resumption of operational capabilities at the original or new permanent location.

2.7. Identification and Authentication – IA

2.7.1. Identification and Authentication (County Users) – IA-2

Information System Owners must:

2.7.1.1 Uniquely identify and authenticate Users or automated Information System processes (Service Accounts) acting on behalf of County Users.

2.7.2. Identification and Authentication (County Users) – Multifactor Authentication to Information System User Accounts IA-2(1)

Information System Owners must:

2.7.2.1 Implement multifactor authentication for access to User Accounts, including both privileged and non-privileged Accounts, when not using the County's Single-Sign-On infrastructure.

2.7.3. Identification and Authentication (County Users) – Access to Accounts – Replay Resistant IA-2(8) (COUNTY ADDED – Not in NIST LOW)

Information System Owners must:

2.7.3.1 Implement replay-resistant authentication mechanisms for access to privileged Accounts.

2.7.4. Identifier Management - IA-4

Information System Owners must:

2.7.4.1 Manage Information System Identifiers by:

1. Receiving authorization from designated personnel to assign an individual, group, role, or device Identifier;
2. Selecting an Identifier that identifies an individual, group, role, or device;
3. Assigning the Identifier to the intended individual, group, role, or device; and
4. Preventing reuse of Identifiers for 180 days.

2.7.5. Authenticator Management - IA-5

Information System Owners must:

2.7.5.1 Manage Information System Authenticators by:

1. Verifying, as part of the initial Authenticator distribution, the identity of the individual, group, role, or device receiving the Authenticator;
2. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;
3. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;
4. Changing/refreshing authenticators every ninety (90) days.

5. Authenticators must be at least eight (8) characters in length and have at least one (1) each of upper and lower-case letters, numbers, and special characters. Users cannot reuse the same password from the past four (4) password cycles.
6. Protecting authenticator content from unauthorized disclosure and modification;
7. Requiring individuals to take, and having devices implement, specific security controls to protect authenticators; and
8. Changing authenticators for group/role accounts when membership to those account changes.

2.7.5.2 For password-based authentication - IA-5(1)

TEBS must:

1. Maintain a list of commonly used, expected, or compromised passwords and update the list annually or when County passwords are suspected to have been compromised directly or indirectly;

Information System Owners must:

2. Verify, when Users create or update passwords, that the passwords are not found on the County-defined list of commonly used, expected, or compromised passwords;
3. Transmit only cryptographically protected passwords;
4. Store passwords using a TEBS-approved hash algorithm
5. Require immediate selection of a new password upon Account recovery;
6. Allow User selection of long passwords and passphrases, including spaces and all printable characters; and
7. Employ automated tools to assist the User in selecting strong password Authenticators.

2.7.6. Authenticator Feedback - IA-6

Information System Owners must:

2.7.6.1 Obscure feedback of authentication information during the authentication process to protect the information from possible exploitation and use by unauthorized individuals.

2.7.7. Cryptographic Module Authentication - IA-7

Information System Owners must:

2.7.7.1 Implement mechanisms for authentication to a Cryptographic Module that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidelines for such authentication.

2.7.8. Identification and Authentication (Non-County Users – Business Partners) IA-8

Information System Owners must:

2.7.8.1 Uniquely identify and authenticate non-County Users or automated Information Systems acting on behalf of non-County Users.

2.7.8.2 Only accept external authenticators that are NIST compliant (as defined in NIST Special Publication 800-63B https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf) and approved by TEBS for all information systems that are accessible to the public (e.g. public-facing websites).

2.7.9. Re-Authentication - IA-11

Information System Owners must:

2.7.9.1 Require Users to re-authenticate when passwords have expired, and new passwords are created.

2.8. Incident Response – IR

2.8.1. Incident Response (IR) Training – IR-2

OEIS Computer Incident Response Team (CIRT) and Department Head/IT Staff must:

2.8.1.1 Provide IR training to team members/coordinators with Incident Response responsibilities;

1. Within 30 days of assuming an incident response role or responsibility, and
2. When required by Information System changes and annually thereafter.

2.8.2. Incident Handling - IR-4

OEIS must:

2.8.2.1 Implement an incident handling capability for security and privacy incidents that includes preparation, detection and analysis, containment, eradication, and recovery;

2.8.2.2 Coordinate incident handling activities with Contingency Planning activities;

2.8.2.3 Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly; and

2.8.2.4 Ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization.

Office of Human Resources (OHR) must:

2.8.2.5 Provide support and direction for sanctions on all events or incidents that involve employees.

2.8.3. Incident Monitoring - IR-5

OEIS must:

2.8.3.1 Track and document Information System security and privacy incidents.

2.8.4. Incident Reporting - IR-6

Information System Owners must:

2.8.4.1 Require personnel to report suspected security and privacy incidents to OEIS within one (1) hour; and

2.8.4.2 Report security, privacy, and supply chain incident information to designated departmental personnel.

OEIS must:

2.8.4.3 Communicate the status of critical incidents to the CAO, Department Directors and/or, to the extent required by applicable laws, notify outside agencies or stakeholders.

2.8.5. Incident Response Assistance - IR-7

OEIS and other Key Players (per the OEIS Incident Response Plan) must:

2.8.5.1 Provide an incident response support resource, integral to the County's incident response capability, that offers advice and assistance to Users of the Information System, for the handling and reporting of security and privacy incidents.

2.8.6. Incident Response Plan - IR-8

OEIS Must:

2.8.6.1 Develop an Incident Response Plan that:

1. Identifies the following:
    a. Preparing for an incident;
    b. Identifying an incident;
    c. Containing the incident;
    d. Eradicating the incident;
    e. Recovering from the incident;
    f. Conducting lessons learned after the incident;
2. Provides guidance for assessing and mitigating the risk of harm to the County and to individuals potentially affected by an incident and/or breach;
3. Outlines procedures for reporting an incident and a breach;
4. Defines reportable incidents;
5. Provides metrics for measuring the incident response capability within the County;
6. Defines the resources and management support needed to effectively maintain and mature an incident response capability; and
7. Is reviewed and approved by designated personnel or roles annually.

2.8.6.2 Distribute copies of the incident response plan to designated incident response personnel within TEBS and Departments;

2.8.6.3 Update the Incident Response Plan to address Information Systems and County changes or problems encountered during plan implementation, execution, or testing;

2.8.6.4 Communicate Incident Response Plan changes to TEBS and Departments; and

2.8.6.5 Protect the Incident Response Plan from unauthorized disclosure and modification.

2.8.6.6 Include the following additional processes in the Incident Response Plan for incidents involving Personally Identifiable Information:

1. A process for notifying affected individuals, if appropriate;
2. An Assessment process to determine the extent of the harm, embarrassment, inconvenience, or unfairness to affected individuals; and
3. A process to ensure prompt reporting by County Users of any privacy incident.

2.9. Maintenance Personnel - MA

2.9.1. Controlled Maintenance – MA-2

Information System Owners must:

2.9.1.1 For non-cloud-based Information Systems:

1. Schedule, document, and review records of maintenance, repair, or replacement on Computer Information Resource Components in accordance with manufacturer or vendor specifications and/or County requirements;
2. Approve and monitor all maintenance activities performed by non-County entities, whether performed on-site or remotely, and whether the Information System or its Components are serviced on-site or removed to another location;
3. Require that designated personnel explicitly approve the removal of the Information System or its Components from County facilities for off-site maintenance, repair, or replacement;
4. Sanitize equipment to remove all information from associated media prior to removal from County facilities for off-site maintenance, repair, or replacement;
5. Check all potentially impacted security and privacy controls to verify that the controls are still functioning properly following maintenance, repair, or replacement actions; and
6. Include in County maintenance records response times for service, if possible, when repairing a network server.

2.9.2. Nonlocal Maintenance – MA-4

Information System Owners must:

2.9.2.1 For non-cloud-based Information Systems:

1. Approve and monitor Nonlocal Maintenance and diagnostic activities performed by the County’s vendors;
2. Allow the use of Nonlocal Maintenance and diagnostic tools only as consistent with County policy;
3. Employ strong Authenticators in the establishment of Nonlocal Maintenance and diagnostic sessions;
4. Maintain records for Nonlocal Maintenance and diagnostic activities; and
5. Terminate session and network connections when Nonlocal Maintenance is completed.

2.9.3. Maintenance Personnel – MA-5

Information System Owners must:

2.9.3.1 Establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel.

2.9.3.2 Verify that all escorted personnel performing maintenance on the Information System possess the required access authorizations; and

2.9.3.3 Designate personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

2.10. Media Protection - MP

2.10.1. Media Access – MP-2

TEBS must:

2.10.1.1 Restrict access to personal devices connected to County Computer Information Resources (i.e. USBs thumb drives, external storage drives, cameras, smart devices, and SD cards).

2.10.1.2 Restrict access to magnetic tape, disk, and documentation libraries to only Users whose responsibilities require access to them.

Information System Owners must:

2.10.1.3 Define types of restricted digital and/or non-digital media and restrict access.

2.10.2. Media Storage – MP-4

Information System Owners must:

2.10.2.1 Physically control and securely store Information System media and protect Information System media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

2.10.3. Media Transport – MP-5

Information System Owners must:

2.10.3.1 Protect and control electronic and non-electronic media during transport outside of controlled areas using protections commensurate with the security category or classification of the information;

2.10.3.2 Maintain accountability for Information System media during transport outside of controlled areas;

2.10.3.3 Document activities associated with the transport of Information System media; and

2.10.3.4 Restrict the activities associated with the transport of Information System media to authorized personnel.

2.10.4. Media Sanitization – MP-5

Information System Owners must:

2.10.4.1 Sanitize Information System media prior to disposal, release out of County control, or release for reuse using TEBS sanitization techniques and procedures;

2.10.4.2 Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

2.10.5. Media Use – MP-7

TEBS must:

2.10.5.1 Restrict/prohibit the use of personal USBs, personal external drives, personal smart devices on Information Systems or Components using defined security safeguards such as Port disabling, Information System scanning, and detection software devices;

2.10.5.2 Prohibit the use of portable storage devices in Information Systems when such devices have no identifiable Owners.

2.11. Physical and Environmental Protection - PE

2.11.1. Physical Access Authorizations – PE-2

Department of General Services and Department of Police Security Services must:

2.11.1.1 Permit only authorized personnel to have access to facilities where systems reside to ensure that access to Information Systems is secure.

Departments must:

2.11.1.2 Develop, approve, review, and maintain a list of individuals with Authorized Access to the facility where the Information System resides.

2.11.1.3 Authorization credentials must be issued for facility access.

2.11.1.4 Review the access list detailing authorized facility access by individuals annually; and

2.11.1.5 Remove individuals from the facility access list when access is no longer required.

2.11.2. Physical Access Control – PE-3

Department of General Services and Department of Police Security Services must:

2.11.2.1 Physically restrict unauthorized personnel from accessing non-public areas of County buildings, computer labs, offices, and work areas containing the Information Systems hardware, including related equipment.

Information System Owners must:

2.11.2.2 Enforce physical access authorizations, safeguards, and maintain physical access Audit Logs at non-public entry and exit points to the facility where the Information Systems hardware resides.

2.11.2.3 Escort visitors and monitor visitor activity in non-public areas.

2.11.2.4 Secure keys, combinations, and other physical access devices;

2.11.2.5 Inventory County defined physical access devices annually;

2.11.2.6 Change combinations and keys when keys are lost, combinations are compromised, or individuals are transferred or terminated.

2.11.3. Monitoring Physical Access – PE-6

Department of General Services and Department of Police Security Services must:

2.11.3.1 Periodically inspect environment and safety of Information Systems by qualified personnel to ensure the safety of Information Systems.

Information System Owners must:

2.11.3.2 Monitor and review physical access to the County facilities where the Information System resides to detect and respond to physical security incidents.

Third-Party Partners Must

2.11.3.3 Monitor and review physical access to Information Systems residing in one or more of their facilities that are either owned or utilized by the County.

2.11.4. Visitor Access Records – PE-8

Information System Owners must:

2.11.4.1 Maintain and review visitor access records to the non-public sections of the County facility where the Information Systems resides.

2.11.5. Emergency Lighting – PE-12

TEBS and the Department of General Services must:

2.11.5.1 Employ and maintain automatic emergency lighting that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

2.11.6. Fire Protection – PE-13

Department of General Services must:

2.11.6.1 Install fire detection and suppression equipment, as required by County, federal, and state law.

2.11.6.2 Employ and maintain fire suppression and detection devices/Information Systems for the Information Systems that are supported by an independent energy source.

Information System Owners must:

2.11.6.3 Ensure alternate work site facilities must be constructed to protect against fire to ensure the safety of County Information.

2.11.7. Temperature and Humidity Controls – PE-14

Department of General Services must:

2.11.7.1 Maintain and monitor temperature and humidity levels within the facility where the Information Systems reside to ensure the safety of the Information Systems.

2.11.8. Water Damage Protection – PE-15

Department of General Services must:

2.11.8.1 Protect the Information Systems from damage resulting from water leakage by providing master shutoff or isolation valves.

Information System Owners must:

2.11.8.2 Ensure that alternate work site facilities protect against water damage to ensure the safety of Information Systems.

2.11.9. Delivery and Removal – PE-16

Information System Owners must:

2.11.9.1 Authorize, monitor, and control Information System Components entering and exiting the facility and maintain records of those items.

2.11.10. Alternate Work Site – PE-17

Departments must:

2.11.10.1 Determine and document the sites allowed for use by employees.

2.11.10.2 Employ the same OEIS security and privacy controls at the alternate work site.

2.11.10.3 Assess as feasible, the effectiveness of security controls at alternate work sites; and

2.11.10.4 Provide a means for employees to communicate with information security and privacy personnel in case of security or privacy incidents or problems.

2.11.11.Emergency Power Control/ Electromagnetic Pulse Protection PE-11/PE-21

Department of General Services must:

2.11.11.1 Use electrical protections and a long-term alternative power supply on Information Systems, commensurate with the importance of the Information System to ensure the safety of Information Systems and personnel.

2.12. Planning - PL

2.12.1. Information Security and Privacy Plans – PL-2

Information System Owners (whose Information Systems store, process, or transmit sensitive data) must:

2.12.1.1 Develop security and privacy plans for the Information System that:

1. Are consistent with the County's and Department's IT enterprise architecture;
2. Explicitly define the authorization boundary for the Information System;
3. Describe the operational context of the Information System in terms of missions and business processes;
4. Provide the security categorization of the Information System including supporting rationale;
5. Describe the operational environment for the Information System and relationships with or connections to other Information Systems;
6. Provide an overview of the security and privacy requirements for the Information System;
7. Identify any relevant overlays, (additional controls or requirements), if applicable;
8. Describe the security and privacy controls in place or planned for meeting those requirements including a rationale for the tailoring decisions; and

9. Are reviewed and approved by a designated official or designated representative prior to plan implementation;

2.12.1.2 Distribute copies of the security and privacy plans and communicate subsequent changes to the plans to TEBS;

2.12.1.3 Review the security and privacy plans at least annually;

2.12.1.4 Update the security and privacy plans to address changes to the Information Systems and environment of operation or problems identified during plan implementation or Security Controls Assessments and Privacy Controls Assessments; and

2.12.1.5 Protect the security and privacy plans from unauthorized disclosure and modification.

2.12.2. Rules of Behavior – PL-4

<u>OEIS and Information System Owners must:</u>

2.12.2.1 Establish and provide to individuals requiring access to the County Information Systems the rules that describe their responsibilities and expected behavior for information and Information Systems usage, security, and privacy;

2.12.2.2 Review and update the Rules of Behavior at least every four (4) years;

2.12.2.3 Require individuals who have read a previous version of the Rules of Behavior to read them again at least every year or when the rules are revised or updated; and

2.12.2.4 Include in the Rules of Behavior explicit restrictions on the use of social media and networking sites and posting organizational information on public websites. Official use of social media on behalf of County government must comply with Administrative Procedure 6-8, “Social Media.”

Personal use of social media on any County-provided computing device is subject to Administrative Procedure 6-1, “Use of County-Provided Technology.” As noted in Administrative Procedure 6-1, all use must comply with all applicable laws and policies.

2.13. Program Management – PM

2.13.1. Information Security Program Leadership Role – PM-2

<u>The County must:</u>

2.13.1.1 Appoint a senior County Information security officer with the mission and resources to develop, implement, and maintain a County-wide information security program.

2.13.2. Information Security and Privacy Resources – PM-3

<u>Departments must:</u>

2.13.2.1 Include the resources needed to implement the information security and privacy programs in County budget planning and investment requests and document all exceptions to this requirement.

2.13.2.2 Prepare documentation required for addressing information security and privacy programs in County budget planning and investment requests in accordance with applicable laws, executive orders, directives, policies, regulations, and standards.

The Office of Management and Budget must:

2.13.2.3 Make available for expenditure, the planned information security and privacy resources.

2.13.3. Plan of Action and Milestones – PM-4

TEBS must:

2.13.3.1 Implement a process to ensure that plans of action and milestones for the information security, privacy, and supply chain risk management programs and associated organizational systems;

1. Are developed and maintained.
2. Remedial information security, privacy, and supply chain risk management actions to adequately respond to risk to organizational operations and assets, individuals, and other organizations are appropriately documented.
3. Are reported in accordance with established laws, regulations, policies, and compliance requirements.

2.13.3.2 Implement a process to ensure that plans of action and milestones for the information security, privacy, and supply chain risk management programs and associated organizational systems;

2.13.4. Information System Inventory – PM-5

TEBS and Information System Owners must:

2.13.4.1 Develop, review, and update, an inventory of information systems and associated reporting requirements on a regularly scheduled basis.

2.13.4.2 Establish, maintain, review, and update an inventory of all systems, applications, and projects that process, store, or transmit personally identifiable information on a regularly scheduled basis.

2.13.5. Measures of Performance – PM-6

TEBS and the County’s Privacy Official must:

2.13.5.1 Develop, monitor, and report on the results of information security and privacy measures of performance.

2.13.6. Enterprise Architecture – PM-7

TEBS must:

2.13.6.1 Develop and maintain an enterprise architecture with consideration for information security, privacy, and the resulting Risk to County operations and assets, individuals, and other organizations.

Information System Owners must:

2.13.6.2 Define functions or services that are not essential to the department's or the County's mission and/or business operations.

2.13.6.3 Offload non-essential functions or services to other systems, system components, or external providers.

2.13.7. Registration Process – PM-10 (COUNTY ADDED)

TEBS must:

2.13.7.1 Manage the security and privacy state of Information Systems and the environments in which those Information Systems operate through Information System registration.

2.13.8. Insider Threat Program – PM-12

TEBS must:

2.13.8.1 Implement an insider threat program that includes a cross-discipline insider threat incident handling team.

2.13.9. Security and Privacy Workforce – PM-13

The County must:

2.13.9.1 Establish a security and privacy workforce development and improvement program.

2.13.10.Contacts with Groups and Associations – PM-15

The County must:

2.13.10.1 establish and institutionalize contact with selected groups and associations within the security and privacy communities:

1. To facilitate ongoing security and privacy education and training for County personnel;
2. To maintain currency with recommended security and privacy practices, techniques, and technologies; and
3. To share current security- and privacy-related information including threats, vulnerabilities, and incidents.

2.13.11.Threat Awareness Program – PM-16

TEBS must:

2.13.11.1 Implement a threat awareness program that includes a cross-organization information sharing capability for threat intelligence.

2.13.12. Accounting of Disclosures – PM-21

The County must:

2.13.12.1 Develop and maintain an Accurate Accounting of disclosures of personally identifiable information, including:

1. Date, nature, and purpose of each disclosure; and
2. Name and address, or other contact information of the person or organization to which the disclosure was made;

2.13.12.2 Retain the accounting of disclosures for the length of the time the personally identifiable information is maintained or five years after the disclosure is made, whichever is longer; and

2.13.12.3 Make the accounting of disclosures available to the individual to whom the personally identifiable information relates upon request.

2.13.13. Minimalization of Personally Identifiable Information Used in Testing, Training, and Research – PM-26

The County must:

2.13.13.1 Develop and implement policies and procedures that address the use of Personally Identifiable Information for internal testing, training, and research;

2.13.13.2 Take measures to limit or minimize the amount of Personally Identifiable Information used for internal testing, training, and research purposes; and

2.13.13.3 Authorize the use of Personally Identifiable Information when such information is required for internal testing, training, and research.

2.13.14. Inventory of Personally Identifiable Information – PM-29

TEBS must:

2.13.14.1 Establish, maintain, and annually update an inventory of all Computer Information Systems and programs that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of Personally Identifiable Information.

2.13.14.2 Use the Personally Identifiable Information inventory to support the establishment of a Continuous Monitoring Program for all new or modified Information Systems containing Personally Identifiable Information.

Information System Owners must:

2.13.14.3 Provide updates of the Personally Identifiable Information inventory to TEBS as needed;

2.13.14.4 Review the Personally Identifiable Information inventory as needed;

2.13.14.5 Ensure to the extent practicable, that Personally Identifiable Information is accurate, relevant, timely, and complete; and

2.13.14.6 Reduce Personally Identifiable Information to the minimum necessary for the proper performance of authorized organizational functions.

2.13.15. Supply Chain Risk Management Strategy – PM-30

The County must:

2.13.15.1 Develop a County-wide strategy for managing supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services;

2.13.15.2 Implement the supply chain risk management strategy consistently across the County; and

2.13.15.3 Review and update, when required, the supply chain risk management strategy on a regularly scheduled basis or as required to address organizational changes.

TEBS and Information System Owners must:

2.13.15.4 Identify, prioritize, and assess suppliers of critical or mission-essential technologies, products, and services.

2.13.16. Continuous Monitoring Strategy – PM-31

The County must:

2.13.16.1 Develop a County-wide continuous monitoring strategy and implement continuous monitoring programs that include:

1. Establishing County-wide metrics that are to be monitored;
2. Establishing frequencies for monitoring and assessing control effectiveness;
3. Establishing ongoing monitoring of organizationally defined metrics in accordance with the continuous monitoring strategy;
4. Correlation and analysis of information generated by control assessments and monitoring;
5. Response actions to address results of the analysis of control assessment and monitoring information; and
6. Reporting the security and privacy status of organizational systems to designated County personnel on an annual basis at a minimum.

2.13.17. Purposing – PM-32

Information System Owners must:

2.13.17.1 For each Information System owned, define, and document all business/County supporting mission-essential services or functions; and

2.13.17.2 On a regularly scheduled basis, analyze supporting mission essential services or functions to ensure that the information resources are being used with their intended purpose.

2.14. Personal Security - PS

2.14.1. Position Risk Designation – PS-2

Departments must:

2.14.1.1 Assign a risk designation to all County positions;

2.14.1.2 Establish screening criteria for individuals filling those positions; and

2.14.1.3 Review and update position risk designations every two years or as frequently as needed.

2.14.2. Personnel Screening – PS-3

Departments must:

2.14.2.1 Screen individuals prior to authorizing access to the Information System.

2.14.2.2 Rescreen individuals in accordance with specific departmental requirements.

2.14.3. Personnel Termination – PS-4

Departments must:

2.14.3.1 Upon termination of User employment:

1. Disable Information System access within the same day;
2. Terminate or revoke any Authenticators and credentials associated with the User;
3. If possible, conduct exit interviews that include a discussion of departmentally defined Information Security topics;
4. Retrieve all security-related County Information System-related property;
5. Retain access to County information and Information Systems formerly controlled by terminated User; and
6. Notify the Help Desk per TEBS policy within same day.

2.14.4. Personnel Transfer – PS-5

Departments must:

2.14.4.1 Review and confirm ongoing operational need for current logical and physical access authorizations to Information Systems and facilities when Users are reassigned or transferred to other positions within the County;

2.14.4.2 Initiate User transfer within the guidelines of the formal OHR transfer action;

2.14.4.3 Modify access authorization, as needed, to correspond with any changes in operational need due to reassignment or transfer; and

2.14.4.4 Notify the Help Desk per TEBS policy within five (5) days of the formal transfer action.

2.14.5. Access Agreements – PS-6

Information System Owners must:

2.14.5.1 Develop and document access agreements for each information system.

2.14.5.2 Review and update the access agreements when appropriate on an annual basis (at a minimum).

2.14.6. Personnel Security – PS-1 & PS7

Departments must:

2.14.6.1 Explicitly define, document, and enforce personnel security requirements for all departmental and contracted personnel.

2.14.6.2 Require all departmental and contracted personnel to comply with personnel security policies and procedures established by the Departments.

2.14.7. Personnel Sanctions – PS-8

Departments must:

2.14.7.1 Employ a formal sanctions process for individuals failing to comply with established information security policies and procedures.

2.14.7.2 Notify OHR within seven (7) days when a formal User sanctions process is initiated, identifying the User sanctioned and the reason for the sanction.

2.15. Risk Assessment - RA

2.15.1. Security Categorization – RA-2

Departments must:

2.15.1.1 Categorize the system and the information it processes, stores, and transmits;

2.15.1.2 Document the security categorization results including supporting rationale, in the security plan for the system; and

2.15.1.3 Verify that the Department head or Department head-designated representative reviews and approves the security categorization decision.

2.15.2. Risk Assessment – RA-3

OEIS must:

2.15.2.1 Conduct a Risk Assessment for new Information System requests, in addition to existing Information Systems that process, store, or transmit County information, and that are appropriately prioritized by OEIS, including the likelihood and magnitude of harm, from

1. The unauthorized or inadvertent access, use, destruction, modification, disclosure, theft, or denial of service of the Information System, the information it processes, stores, or transmits, and any related information; and
2. Privacy-related issues for individuals arising from the intentional processing of Personally Identifiable Information;

2.15.2.2 Integrate Risk Assessment results and risk management decisions from the County and missions/business process perspectives with Information System-level Risk Assessments;

2.15.2.3 Document Risk Assessment results in Risk Assessment reports;

2.15.2.4 Review Risk Assessment results annually;

2.15.2.5 Disseminate Risk Assessment results to respective Information System Owners; and

2.15.2.6 Update the Risk Assessment every 4 (four) years or when there are significant changes to the Information System, its environment of operation, or other conditions that may impact the security or privacy state of the Information System.

2.15.3. Vulnerability Monitoring and Scanning of Information Systems – RA-5

OEIS must:

2.15.3.1 Monitor and Scan for vulnerabilities in the system(s) and hosted applications in accordance with County-defined frequencies, randomly and/or when new vulnerabilities potentially affecting the system(s) are identified and reported.

1. Where and when feasible, implement tools capable of monitoring, detecting, and acting on security threats on County Information Systems and hosted applications daily.

2. Scan all County assets monthly at minimum and when new vulnerabilities potentially affecting County Information Systems are identified and reported.

3. Perform an internal/external information security/privacy audit, assessment, and/or penetration test on at least one County Information System and/or Hosted Application annually.

2.15.3.2 Employ Vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the Vulnerability management process by using standards for:

1. Enumerating platforms, software Flaws, and improper configurations;
2. Formatting checklists and test procedures; and
3. Measuring Vulnerability impact;

2.15.3.3 Employ Vulnerability scanning tools that include the capability to readily update the vulnerabilities to be scanned.

Departments must:

2.15.3.4 Analyze Vulnerability scan reports and results from Security Controls Assessments;

2.15.3.5 Remediate legitimate vulnerabilities in accordance with the County's assessment of risk;

1. **Critical/High Severity** - Immediately assign resources possessing the skill sets required to identify/implement required mitigation/resolution strategies, ensuring that the appropriate level of urgency is maintained to ensure that the mitigation/resolution of findings occurs in the least amount of time possible.
2. **Moderate/Medium** - Remediate findings thirty (30) calendar days from the date on which the Department was notified of the finding.
3. **Low Risk** - Remediate findings ninety (90) calendar days from the date on which the Department was notified of the finding.

2.15.3.6 Share information obtained from the Vulnerability scanning process and Security Controls Assessments with OEIS to help eliminate similar Vulnerabilities in other Information Systems.

TEBS must:

2.15.3.7 Establish a public-facing reporting channel for receiving reports of vulnerabilities in organizational systems and system components.

2.15.4. Risk Response – RA-7

All (Information System Owners, Departments, Management, and CAO) Must:

2.15.4.1 Respond to findings from security and privacy assessments, monitoring, and audits in accordance with organizational Risk Tolerance (The level of risk or the degree of uncertainty that is acceptable to an organization – NIST SP 800-53 Rev 5 https://doi.org/10.6028/NIST.SP.800-53r5).

Risk Response is defined (NIST SP 800-53 Rev 5 - https://doi.org/10.6028/NIST.SP.800-53r5) as accepting, avoiding, mitigating, sharing, or transferring risk to organizational operations (mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. The County also recognizes 'dispute' as an acceptable response.

2.15.4.1.1 Risk Acceptance

Although NIST does not define Risk Acceptance it is commonly known as the deliberate decision by an organization or individual to accept the potential negative consequences of a risk, without taking further action to mitigate or avoid it. It involves acknowledging that a particular risk exists, assessing its potential impact, and determining that the potential benefits or advantages outweigh the associated risks.

All Must:

2.15.4.1.1.1 Initially accept risk(s) that have been transferred to them based upon existing documentation identifying the individual/department as the owner of the asset(s) associated with the risk(s).

M3 Level Management (Corresponding Level of Uniformed Manager) May:

2.15.4.1.1.2 Decide to accept "Low" severity risks(s) transferred to them along with the potential negative consequences of the risk(s), without taking further action to mitigate or avoid it after assessing its potential impact, determining that the potential benefits or advantages outweigh the associated risks and that the risk falls within the department's Risk Tolerance.

M2 Level Management (Corresponding Level of Uniformed Manager) May:

2.15.4.1.1.3 Decide to accept "Medium/Moderate" severity risks(s) transferred to them along with the potential negative consequences of the risk(s) without taking further action to mitigate or avoid it after assessing its potential impact, determining that the potential benefits or advantages outweigh the associated risks, and determining that the risk falls within the department's Risk Tolerance.

M1 Level Management (Corresponding Level of Uniformed Manager) May:

2.15.4.1.1.4 Decide to accept "High" severity risks(s) transferred to them along with the potential negative consequences of the risk(s), without taking further action to mitigate or avoid it after assessing its potential impact, determining that the potential benefits or advantages outweigh the associated risks and that the risk falls within the department's Risk Tolerance.

CIO Must:

2.15.4.1.1.5 Accept risks under the following circumstances:

TEBS fails to perform a Risk Assessment

TEBS fails to document, and/or not appropriately communicate risks identified because of an audit, risk assessment and/or penetration test.

TEBS fails to submit a budget request required to mitigate the risk(s)

The CIO fails to champion a budget request required to mitigate the risk(s)

CAO May:

2.15.4.1.1.6 Decide to accept "Critical" severity risks(s) transferred to them along with the potential negative consequences of the risk(s), without taking further action to mitigate or avoid it after assessing its potential impact, determining that the potential benefits or advantages outweigh the associated risks and that the risk falls within the department's Risk Tolerance.

CAO Must:

2.15.4.1.1.7 Accept risk along with the potential negative consequences of the risk(s), regardless of severity level when the CAO denies a funding request submitted by OMB.

OMB Must:

2.15.4.1.1.8 Accept risk along with the potential negative consequences of the risk(s), regardless of severity level when a submitted funding request is denied.

2.15.4.1.2 Risk Mitigation

Risk Mitigation is defined (NIST SP 800-53 Rev 5 - https://doi.org/10.6028/NIST.SP.800-53r5) as prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process.

All Must:

2.15.4.1.2.1 Diligently employ all reasonable measures to mitigate risks.

2.15.4.1.3 Risk Sharing

Although NIST does not define Risk Sharing it is commonly known as the strategy or approach in which an organization transfers or shares a portion of its risks with another party. It involves distributing the potential negative consequences of a risk across multiple entities or stakeholders, typically through contractual agreements, insurance policies, or partnerships.

All Must:

2.15.4.1.3.1 Share risk(s) based on contractual agreements, insurance policies and/or established partnerships when and where appropriate.

2.15.4.1.4 Risk Transfer

Although NIST does not define Risk Transfer, guidance is provided in NIST SP 800-37 where Risk Transfer is described as a risk response option where the organization shifts the financial or operational burden of a risk to another entity. This is typically accomplished through mechanisms such as contracts, insurance policies, or outsourcing arrangements. For the intent and purpose of this document, Risk Transfer includes the transfer of risk(s) from one County entity to another based on asset ownership and/or the denial of funding requests.

OEIS Must:

2.15.4.1.4.1 Transfer risk(s) to the department owning the Assets associated with the risk(s) via formal risk notification within a reasonable time following the notification of newly discovered risk.

Management Must:

2.15.4.1.4.2 Transfer risk(s) according to the following:

To the OEIS if after Risk Acceptance, it has been determined that the Assets associated with the risk(s) are not owned by the department.

To OMB via formal notification when funding requests required to mitigate the risk(s) have been denied.

OMB Must:

2.15.4.1.4.4 Transfer risk(s) to the CAO via formal notification when funding requests submitted to the CAO are denied.

2.15. Information System and Services Acquisition - SA

2.15.5. Allocation of Resources – SA-2

The County must:

2.15.5.1 Determine information security and privacy requirements for the Information Systems or services in County in mission and business process planning;

2.15.5.2 Determine, document, and allocate the resources required to protect the Information Systems or service as part of the County capital planning and investment control process; and

2.15.5.3 Establish a discrete line item for information security and privacy in County programming and budgeting documentation.

2.15.6. Information System Development Life Cycle – SA-3

Information System Owners must:

2.15.6.1 Manage the Information System using Information System Development Life Cycle processes that incorporate information security and privacy considerations;

2.15.6.2 Define and document information security and privacy roles and responsibilities throughout the Information System Development Life Cycle;

2.15.6.3 Identify individuals having information security and privacy roles and responsibilities; and

2.15.6.4 Integrate the County's information security and privacy risk management process into Information System Development Life Cycle activities.

2.15.7. Acquisition Process – SA-4

The County must:

2.15.7.1 include the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the Information System, Component, or service:

1. Security and privacy functional requirements;
2. Strength of mechanism requirements, including degree of correctness, completeness, resistance to tampering or bypass, and resistance to direct attack.
3. Security and privacy assurance requirements;
4. Security and privacy documentation requirements;
5. Requirements for protecting security and privacy documentation;
6. Description of the Information System development environment and environment in which the Information System is intended to operate;
7. Allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain Risk management; and
8. Acceptance criteria.

2.15.8. Information System Documentation – SA-5

Information System Owners must:

2.15.8.1 Obtain administrator documentation for the Information System, Component, or service that describes:

1. Secure configuration, installation, and operation of the Information System, Component, or service;

2. Effective use and maintenance of security and privacy functions and mechanisms; and
3. Known vulnerabilities regarding configuration and use of administrative or privileged functions;

2.15.8.2 Obtain User documentation for the Information System, Component, or service that describes:

1. User-accessible security and privacy functions and mechanisms and how to effectively use those functions and mechanisms;
2. Methods for User interaction, which enables individuals to use the Information System, Component, or service in a more secure manner and protect individual privacy; and
3. User responsibilities in maintaining the security of the Information System, Component, or service and privacy of individuals;

2.15.8.3 Document attempts to obtain Information System, Information System Component, or Information System service documentation when such documentation is either unavailable or nonexistent.

2.15.8.4 Protect documentation as required, in accordance with the County's Risk management strategy; and

2.15.8.5 Distribute documentation to Department Heads and TEBS OEIS.

2.15.9. Security and Privacy Engineering Principles – SA-8

Information System Owners must:

2.15.9.1 Apply OEIS security and privacy engineering principles, as defined in TEBS architecture documents, in the specification, design, development, implementation, and modification of the Information System and components.

2.15.10.External System Services – SA-9

Contractors and the County must:

2.15.10.1 If a contractor's personnel will access County information systems as part of its performance, the parties must attach and incorporate by reference into the contract Administrative Procedure ("AP") 6-7, Information Resource Security. AP 6-7.

Contractors must:

2.15.10.2 Acknowledge and advise its personnel who provide information system configuration services that;

1. The County follows the ISSADOH and NIST Special Publication (SP) 800-53 (rev. 5); or
2. The ISSADOH Handbook requires system owners to set or comply with articulated rules for: system, general data, and sensitive information access; user authentication; system maintenance and updates, audits; system configuration maintenance and modification (for both local and cloud-based systems); contingency in the event of system failure; data backup; security incident notification; physical access to facilities housing systems; transportation of system media and components; reporting of security incidents; and remediation of security vulnerabilities.

2.15.10.3 Acknowledge that any system design, configuration, customization, or implementation must comport with County information security and privacy engineering principles and the County's information system architecture.

Contractor Personnel must:

2.15.10.4 Comply with the "Rules of Behavior" which is an Appendix to AP 6-7 when accessing County information systems with a County-assigned user identification.

County Information System Owners must:

2.15.10.5 Comply with the "Information Security System and Data Owners' Handbook (ISSADOH)" which is an Appendix to AP 6-7. The ISSADOH adopts and is consistent with NIST Special Publication 800-53 (rev. 5).

Cloud Contracts:

Contractors must:

2.15.10.6 Be minimally certified as FedRAMP Low; or

2.15.10.7 NIST 800-53 certified or compliant via a third-party assessment.

2.15.11. Unsupported Information System Components – SA-22

Information System Owners must:

2.15.11.1 Replace Information System Components when support for the components is no longer available from the developer, vendor, or manufacturer.

2.16. Information System and Communications Protection - SC

2.16.1. Denial of Service Protection – SC-5

TEBS must:

2.16.1.1 Protect against or limit the effects of Denial-of-Service events by employing security safeguards.

2.16.2. Boundary Protection – SC-7

TEBS must:

2.16.2.1 Monitor and control communications at the external boundary of the Information System and at key internal boundaries within the Information System;

2.16.2.2 Implement subnetworks for publicly accessible Information System Components that are separated from internal County networks; and

2.16.2.3 Connect to external networks or Information Systems only through managed interfaces consisting of Boundary Protection Devices arranged in accordance with County security and privacy architecture.

2.16.3. Cryptographic Key Establishment and Management – SC-12

Information System Owners must:

2.16.3.1 Establish and manage Cryptographic Keys for required cryptography employed within a Information System in accordance with OEIS requirements for key generation, distribution, storage, access, and destruction.

2.16.4. Cryptographic Protection – SC-13

<u>TEBS must:</u>

2.16.4.1 Implement defined cryptographic uses and type of cryptography for each use to ensure cryptographic protection of data.

2.16.5. Collaborative Computing Devices and Applications – SC-15

<u>TEBS must:</u>

2.16.5.1 Prohibit remote activation of Collaborative Computing devices and applications with exceptions (if applicable); and

2.16.5.2 Provide an explicit indication of use to Users physically present at the devices.

2.16.6. Secure Name/Address Resolution Service – SC-20 & SC-21

<u>TEBS must:</u>

2.16.6.1 Utilize a secure name server (DNS) where zone administration is conducted. The name of a server should not be identified as a "name server" and should not be accessible via the internet.

2.16.6.2 Provide the means to indicate the security status of networking zones.

2.16.7. Architecture and Provisioning for Name/Address Resolution Service – SC-22

<u>Information System Owners must:</u>

2.16.7.1 Ensure that information systems that collectively provide name/address resolution services for the County are fault tolerant (elimination of single-points-of-failure) and implement internal/external role separation.

2.16.8. Process Isolation – SC-39

2.16.8.1 Maintain a separate execution domain for each executing process with the system.

2.17. Information System and Information Integrity - SI

2.17.1. Flaw Remediation – SI-2

<u>Information System Owners must:</u>

2.17.1.1 Identify, report, and correct Information System Flaws;

2.17.1.2 Test software and firmware updates related to Flaw remediation for effectiveness and potential side effects before installation;

2.17.1.3 Install security-relevant software and firmware updates immediately upon notification from OEIS of High Vulnerabilities. Moderate-Risk Vulnerabilities must be updated within thirty (30) days from the date of discovery and Low Risk Vulnerabilities mitigated within ninety (90) days and;

2.17.1.4 Incorporate Flaw remediation into the TEBS configuration management process.

2.17.2. Malicious Code Protection – SI-3

<u>TEBS and Information System Owners must:</u>

2.17.2.1 Implement Signature Based, and/or Non-signature Based Malicious Code protection mechanisms at Information System network entry and exit points to detect and eradicate Malicious Code;

2.17.2.2 Automatically update Malicious Code protection mechanisms whenever new releases are available in accordance with TEBS configuration management policy and procedures;

2.17.2.3 Configure Malicious Code protection mechanisms to:

1. Perform periodic scans of the Information System and real-time scans of files from external sources at endpoints and/or network entry/exit points as the files are downloaded, opened, or executed in accordance with County policy; and
2. Block Malicious Code; and/or quarantine Malicious Code; and/or send an alert to the administrator; promptly in response to Malicious Code detection; and

2.17.2.4 Address the receipt of false positives during Malicious Code detection and eradication and the resulting potential impact on the availability of the Information System.

2.17.3. Information System Monitoring – SI-4

<u>OEIS and Information System Owners must:</u>

2.17.3.1 Monitor the Information System to detect:

1. Attacks and indicators of potential attacks; and
2. Unauthorized local, network, and remote connections;

2.17.3.2 Identify unauthorized use of the Information System;

2.17.3.3 Invoke internal monitoring capabilities or deploy monitoring devices:

1. Strategically within the Information System to collect County-determined essential information; and
2. At ad hoc locations within the Information System to track specific types of transactions of interest to the County;

2.17.3.4 Protect information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;

2.17.3.5 Adjust the level of Information System monitoring activity when there is a change in Risk to County's operations and assets, individuals, other organizations, or the Nation;

2.17.3.6 Ensure Information System monitoring complies with all applicable County policies/procedures, Federal, State, and Local laws; and

2.17.3.7 Provide Information System monitoring information to OEIS.

2.17.4. Security Alerts, Advisories, and Directives – SI-5

<u>OEIS must:</u>

2.17.4.1 Receive Information System security alerts, advisories, and directives on an ongoing basis;

2.17.4.2 Generate internal security alerts, advisories, and directives as deemed necessary; and

2.17.4.3 Disseminate security alerts, advisories, and directives to: Users, Information System security personnel, and administrators with configuration/patch management responsibilities.

Information System Owners must:

2.17.4.4 Implement security directives in accordance with established timeframes, or

2.17.4.5 Notify OEIS of the degree of noncompliance.

2.17.5. Information Management and Retention – SI-12

Information System Owners must:

2.17.5.1 Manage and retain information within the Information System and information output from the Information System in accordance with applicable laws, Executive Orders, directives, regulations, policies, standards, guidelines, and operational requirements.

2.18. Supply Chain Risk Management - SR

2.18.1. Supply Chain Risk Management Plan – SR-2

TEBS and Information System Owners must:

2.18.1.1 Develop a Supply Chain Risk Management Plan (SCRM) plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of defined systems, system components, or system services.

2.18.1.2 Review and update, as required, the supply chain risk management plan on a regularly scheduled basis.

2.18.1.3 Establish a supply chain risk management team consisting of personnel, roles, and responsibilities to lead and support defined SCRM activities.

2.18.2. Supply Chain Controls and Processes – SR-3

TEBS and Information System Owners must:

2.18.2.1 Establish a process or processes to identify and address weaknesses or deficiencies in the supply chain elements and processes of defined system(s) or system(s) component(s)

2.18.2.2 Employ defined controls to protect against supply chain risks to the system, system component, or system service and to limit the harm or consequences from supply chain related events: and

2.18.2.3 Document the selected and implemented supply chain processes and controls in the supply chain risk management plan.

2.18.3. Acquisition Strategies, Tools, and Methods – SR-5

The County must:

2.18.3.1 Employ the defined acquisition strategies, contract tools, and procurement methods to protect against, identify, and mitigate supply chain risks.

2.18.3.2 Employ defined controls (e.g., use of multiple suppliers throughout the supply chain for the identified critical components, stockpiling spare components to ensure operation during mission-critical times, and the identification of functionally identical or similar components that may be used, if necessary) to ensure adequate supplies of defined critical system components.

2.18.4. Anti-Counterfeit Training – SR-11

TEBS and Information System Owners must:

2.18.4.1 Train defined County personnel on how to detect counterfeit system components (including hardware, software, and firmware).

2.18.4.2 Maintain configuration control over defined system components awaiting service or repair and serviced or repaired components awaiting return to service.

2.18.5. Component Disposal – SR-12

TEBS and Information System Owners must:

2.18.5.1 Dispose of data, documentation, tools, or system components utilizing the appropriate, defined techniques and methods.

2.19. Exemption from Administrative Procedure

A Department may be exempt from the AP 6-7 Administrative Procedure under the following conditions:

2.19.1.1 Information security awareness training – a Department may request exemptions for specific employees due to resource limitations or conflicts for up to one (1) year. A Department head may request exemptions for non-employees (such as contractors or volunteers) who completed comparable training elsewhere within the past year. Exemption requests must be submitted to the OEIS, and the Department Head must assume the risk.

3. APPENDICES

3.1. Definitions

TERM:	DESCRIPTION:
Account Manager	An Account Manager is a System Administrator role with specific duties to create, enable, modify, disable and remove user and service accounts in accordance with Montgomery County policy, procedures, and conditions.
Accurate Accounting of Disclosure	The precise process of recording, summarizing, analyzing, and reporting of Personally Identifiable Information (PII) disclosure information to include; the date, nature, and purpose of each disclosure of record, in addition to, the name and address of the person or agency to which the disclosure was made.
Alternate Storage Site	An Alternate Storage Site is geographically distinct from a primary storage site. An Alternate Storage Site maintains duplicate copies of information and data that can be readily retrieved if the primary storage site becomes unavailable.
Assessment	See Security Assessment or Privacy Assessment
Assessor	The individual, group, or organization responsible for conducting Security and Privacy Controls Assessments.
Audit Event	An Audit Event is any observable security-relevant occurrence in an organizational Information System.
Authorized Access	Access privileges granted to a User, program, or process or the act of granting those privileges.
Audit Log	A chronological record of Information System activities, including records of Information System accesses and operations performed during a given period
Audit Record	An individual entry in an Audit Log related to an audited event.
Audit Trail	A chronological record that reconstructs and examines the sequence of activities surrounding or leading to a specific operation, procedure, or event in a security-relevant transaction from inception to result.
Authenticator	The means used to confirm the identity of a User, processor, or device (e.g., User password or token).
Authorization Boundary	All components of an information system to be authorized for operation. This excludes separately authorized systems to which the information system is connected.
Baseline Configuration	A documented set of specifications for an Information System, or a configuration item within an Information System, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures. Baseline Configurations serve as a basis for future builds, releases, and/or changes to Information Systems. Baseline Configurations include information about Information System components, network topology, and the logical placement of those components within the Information System architecture. (for more information see NIST SP 800-128)
Boundary Protection	Monitoring and control of communications at the external boundary of an Information System to prevent and detect malicious and other unauthorized communications, using Boundary Protection Devices, for example, gateways, routers, firewalls, guards, encrypted tunnels.

TERM:	DESCRIPTION:
Boundary Protection Device	A device with appropriate mechanisms that facilitates the adjudication of different interconnected Information System security policies or provides Information System Boundary Protection.
Change Monitoring	A process that identifies and tracks changes to County Information Systems and environments of operations that may affect security and privacy risks.
Compliance Monitoring	A process that verifies that the required Risk Response measures are implemented. It also verifies that security and privacy requirements are satisfied.
Component	A discrete identifiable information technology asset that represents a building block of an Information System and may include hardware, software, and firmware.
Computer Information Resource	Hardware, software, websites, web-based services, and databases
Configuration Settings	Configuration Settings are the parameters that can be changed in hardware, software, or firmware Components of the Information System and affect the security posture or functionality of the Information System.
Collaborative Computing	An interactive multimedia conferencing application that enables multiple parties to collaborate on textual and graphic documents. Collaborative Computing devices and applications include, for example, remote meeting devices and applications, networked white boards, cameras, and microphones.
Compliance-Mandated Departments or Information Systems	Departments or Information Systems that process, store, and/or transmit data subject to security restrictions imposed by the Federal, State or Local Government contracts, such as, Health Insurance Portability and Accountability Act (HIPAA), FBI Criminal Justice Information Services Division (FBI CJIS), and the Payment Card Industry Data Security Standard (PCI-DSS).
Contingency Planning	Contingency Planning for Information Systems is part of an overall organizational program for achieving continuity of operations for mission/business functions. Contingency Planning addresses Information System restoration and implementation of alternative mission or business processes when Information Systems are compromised, breached, or destroyed
Control Baseline	The set of minimum security and privacy controls defined for a system or selected based on the privacy selection criteria that provide a starting point for the tailoring process. (For more information, see FIPS 200)
Controls	**See Security Controls**
Controls Assessment	**See Security Controls Assessment**
Countermeasures	Actions, devices, procedures, techniques, or other measures that reduce the Vulnerability of a system. Synonymous with **Security Controls and Safeguards**. (For more information, see FIPS 200)
Cryptographic Key	A Cryptographic Key is a technical method used to transform data from normal plain information to encrypted information that is no longer readable.
Cryptographic Module	A Cryptographic Module is defined as any combination of hardware, firmware or software that implements cryptographic functions such as encryption, decryption, digital signatures, authentication techniques or random number generation.
Denial of Service	A Denial-of-Service attack is a malicious security event that occurs when an attacker takes action that prevents legitimate Users from accessing targeted computer Information Systems, devices, or other network resources.
Effectiveness Monitoring	A process that determines the ongoing efficiency of implemented Risk Response measures.

TERM:	DESCRIPTION:
Execution Domain	An Execution Domain is a mechanism to isolate executed software applications from one another so that they do not affect each other; one process cannot modify the executing code of another process.
External Information System	Systems or components of systems that are outside of the authorization boundary established by the County and for which the County typically has no direct supervision and authority over the application of required security controls or the assessment of control effectiveness. This includes systems managed by contractors, systems owned by federal agencies, and systems owned by other entities. This control addresses the use of external systems for the processing, storage, or transmission of County information, including, for example, accessing cloud services from County systems.
Flaw	A Flaw is a weakness in an Information System's design, implementation or operation and management that can be exploited to violate the Information System's security policy.
Full Backups	A Full Backup is a backup of the Information Systems that contains all the data in the folders and files that are selected to be backed up.
High Risk	A High Risk could be expected to have a severe or catastrophic adverse effect on the County's operations, assets, or individuals. Corrective actions must be implemented as soon as possible.
Identifier	Unique data used to represent a person's identity and associated attributes. It may be an identifying name, card number, or may be something more abstract (for example, a string consisting of an IP address and timestamp), depending on the Information System.
Incident (Security)	1. An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.
Incremental Backups	An Incremental Backup is a backup of the Information System that contains only those files that have been altered since the last Full Backup (e.g. following a Full Back up on Friday, a Monday backup will contain only those files that changed since Friday. A Tuesday backup contains only those files that changed since Monday, and so on)
Information Security	The protection of information and systems from unauthorized or inadvertent access, use, destruction, modification, disclosure, theft, or denial of service.to provide confidentiality, integrity, and availability.
Information Steward	A County Information System security role with statutory or operational authority for information, governance processes, and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.
Information System	NIST: A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information, whether such information is in digital or non-digital form.
Information System Account Manager	A System Administrator role with specific duties to create, manage, disable and delete user, privileged user, and service accounts.

TERM:	DESCRIPTION:
Information System-Level Information	The operating Information System or some other controls program information, for example, Information System state information, operating Information System type, application software, and licenses
Information System Owner	Individual responsible for the overall security, budgeting, procurement, development, integration, modification, or operation and maintenance of an Information System.
Information Type	A specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor-sensitive, security management) defined by an organization or in some instances, by a specific law, Executive Order, directive, policy, or regulation. (For more information see FIPS 199)
Interconnection Security Agreements (ISA)	A document that regulates security-relevant aspects of an intended connection between the County and an External Information System. It regulates the security interface between any two Information Systems operating under two different distinct authorities. It includes a variety of descriptive, technical, procedural, and planning information. It is usually preceded by a formal Memorandum of Agreement (MOA)/Memorandum of Understanding (MOU) that defines high-level roles and responsibilities in management of a cross-domain connection.
Least Privilege	A security principle that restricts the access privileges of authorized personnel to the minimum Information System resources and authorizations that the User needs to perform its function.
Logical Access	Interactions with hardware through Remote Access. This type of access generally features identification, authentication, and authorization Protocols.
Low Risk	A Low Risk could be expected to have a limited adverse effect on the County's operations, assets or individuals.
Malicious Code	Software or firmware computer code or script intended to perform an unauthorized process that will have an adverse impact on the confidentiality, integrity, or availability of an Information System. A virus, worm, Trojan horse, back door, or other code-based threat that infects a host. Spyware and some forms of adware are also examples of Malicious Code.
Malicious Code Protection Mechanisms (Non-signature Based Malicious Code and Signature Based Code Protection)	Hardware and/or software designed to prevent the execution of Malicious Code. Signature Based Malicious Code detection relies on previous identification to prevent "known" Malicious Code. Non-signature based Malicious Code detection uses behavior-based analysis to prevent "unknown" Malicious Code.
Moderate Risk	A Moderate Risk could be expected to have a serious adverse effect on the County's operations, assets, or individuals.
Nonlocal Maintenance	Nonlocal Maintenance and diagnostic activities are those activities conducted by individuals communicating through a network, either an external or internal network.
Multi-Factor (Two Factor) Authentication	Authentication using two or more factors to achieve authentication. Factors include: (i) something you know (e.g., password/personal identification number (PIN)); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric).
Office of Enterprise Information Security (OEIS)	An office within TEBS that is responsible for the security of the County's Information System(s).

TERM:	DESCRIPTION:
Peer-to-Peer (P2P) File Sharing Technology	P2P file sharing allows users to access media files such as books, music, movies, and games using a P2P software program that searches for other connected computers on a P2P network to locate the desired content. Examples: iTunes, Napster or BitTorrent.
Penetration Testing	A test methodology in which assessors, typically working under specific constraints, attempt to circumvent or defeat the security features of a system.
Personally, Identifiable Information	Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.
Ports	A computer Port is a connection point or interface between a computer and an external or internal device. Internal Ports may connect such devices as hard drives and CD ROM or DVD drives; external Ports may connect modems, printers, mice, and other devices.
Privacy Controls Assessment Plan	The objectives for Privacy Controls Assessments and a detailed roadmap of how to conduct such assessments.
Privacy Controls Assessments	The testing or evaluation of privacy controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the privacy requirements for an Information System.
Protocol	A Protocol is a set of rules or procedures for transmitting data between electronic devices, such as computers.
Remote Access	Remote access to an Information System by a User (or an automated Information System acting on behalf of a User) communicating through an external network.
Replay Resistant	Protection against the capture of transmitted authentication or access control information and its subsequent retransmission with the intent of producing an unauthorized effect or gaining unauthorized access
Risk Acceptance	Accepting risk occurs when an Information System Owner acknowledges that the potential loss from a risk is not great enough to warrant spending money to avoid or mitigate it.
Risk Assessment	The process of identifying risks to County operations (including mission, functions, image, reputation), assets, personnel, or residents, resulting from the operation of an Information System. Risk Assessment is part of risk management and incorporates threat/Vulnerability analyses, and considers mitigations provided by security controls planned or in place.
Risk Avoidance/Rejection	Risk Avoidance is the elimination of hazards, activities, and exposures that can negatively affect the County's assets.
Risk Mitigation	Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process. A systematic reduction in the extent of exposure to a risk and/or the likelihood of its occurrence.
Risk Response	Accepting, avoiding, mitigating, transferring, or rejecting risk to County operations, assets, or residents.
Risk Sharing/Transfer	A strategy that involves the contractual shifting of a risk from one party to another.

TERM:	DESCRIPTION:
Role-Based Access Control	Access control based on user roles (i.e., a collection of access authorizations a user receives based on an explicit or implicit assumption of a given role). Role permissions may be inherited through a role hierarchy and typically reflect the permissions needed to perform defined functions within an organization. A given role may apply to a single individual or to several individuals
Secure Name Server	A secure domain name server, or DNS server, is an Internet protocol that turns URLs like (https://www.montgomerycountymd.gov/) into IP addresses (like 192.168.18.29) that are used by internal County servers to identify each other on the network.
Security Controls Assessment Plan	The objectives for Security Controls Assessments and a detailed roadmap of how to conduct such assessments.
Security Controls Assessment	The testing or evaluation of security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for an Information System.
Security Controls	Actions that are taken as a matter of process, procedure or automation that reduce security risks. Diverse requirements derived from mission and business needs, laws, Executive Orders, directives, regulations, policies, standards, and guidelines.
Security Impact Analysis	The analysis conducted by an organizational official to determine the extent to which changes to the system have affected the security state of the system.
Security Plan (AKA System Security Plan)	Formal document that provides an overview of the security requirements for an information system or an information security program and describes the security controls in place or planned for meeting those requirements. The system security plan describes the system boundary; the environment in which the system operates; how the security requirements are implemented; and the relationships with or connections to other systems.
Sensitive Information	Any information that by law or County policy that cannot publicly be disclosed, including without limitation: A. Non-Public criminal justice information. B. Credit or debit card numbers. C. An individual’s first name or first initial and last name, name suffixes, or unique biometric or genetic print or image, in combination with one or more of the following data elements. a) A Social Security numbers. b) A driver’s license number or state identification card number, or other individual identification number issued by a state or local government. c) Passport number or other identification number issued by the United States government. d) An Individual Taxpayer Identification Number. e) A financial or other account number that in combination with any required security code, access code, or password, would permit access to an individual’s account. f) Medical records; or g) Health insurance information.

TERM:	DESCRIPTION:
Service Account	A special User account that an application or service uses to interact with the operating system. Services use the service accounts to log on and make changes to the operating system or the configuration. For example, if certain criteria are established on a device, then an action or service will occur. Service Accounts are used for many enterprise applications.
System Development Life Cycle (SDLC)	A framework defining tasks performed at each step (Requirements, Design, Implementation, Verification, Maintenance) in the software development process.
Tailoring	The process by which security Control Baselines are modified by identifying and designating common controls; applying scoping considerations on the applicability and implementation of baseline controls; selecting compensating security controls; assigning specific values to organization-defined security control parameters; supplementing baselines with additional security controls or control enhancements; and providing additional specification information for control implementation
Technology & Enterprise Business Solutions (TEBS)	An Executive Branch Department that is responsible for County Government enterprise Information Systems and telecommunications.
User or Information System User	Any appropriately provisioned individual with a requirement to access a County information system. County User – A County employee, contractor, or volunteer that has access to County information systems by virtue of being provisioned an active directory account. Non-organizational User – A user who is not a County user (including public users).
User Account	An established relationship between a User and a computer, network, or information service.
User-Level Information	Data that is created or consumed by the User on the Information System.
Vulnerability	A weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.
Vulnerability Assessment	Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.
Wireless Access	Telecommunications in which electromagnetic waves (rather than some form of wire) carry the signal over part or all the communication paths.