Open Solicitation Plan
For
Open Solicitation #1161701 - Animal Behaviorist Services

As required by Montgomery County Procurement Regulations, Code of Montgomery County (the "County") Regulations (COMCOR), Section 11B.00.01, et seq., Section 4.1.6.3 (a), the Office of Animal Services submits this Open Solicitation Plan for approval by the Director, Office of Procurement, Montgomery County, Maryland.

Section 4.1.6.3 Procedure

1. Public Notice — Notice for this solicitation will be posted on the County Office of Procurement website.
2. Application Process — The Office of Animal Services (OAS) Team will mail out the solicitation packet for this Open Solicitation to all providers who express an interest in applying to provide the services. The solicitation packet includes the following: 1) the Notice to Vendors that summarizes this Open Solicitation; 2) the Instructions to Vendors; and 3) the pre-approved Form Contract including the Scope of Services and General Conditions of Contract Between County and Contractor and other attachments. Applicants will be required to sign the Application Form (Attachment B) to the Pre-Approved Form Contract stating that they have received the solicitation packet and understand the requirements of this Open Solicitation.
3. Criteria for accepting or rejecting applications — The Pre-Approved Form Contract contains the minimum qualifications for services upon which applicants will be accepted. Applications will be reviewed by OAS staff for acceptance or rejection, based on the minimum qualifications.
4. All applicants meeting the minimum qualifications listed in the Pre-Approved Form Contract will be eligible to receive a contract to provide the services described in the Open Solicitation. The selected providers will be placed on the list of current contracts for the Montgomery County Office of Animal Services and will be selected to provide services based on necessity on an "as needed" basis. Work assignments will be made on a rotating basis in the order in which the contracts are executed, unless a unique skill set is required, in which case the County may contact the provider with the unique skills required for a particular assignment, even if that provider is not up next in the rotation. For example, if five contracts are executed because of this Open Solicitation, the County would contact Provider A for the first assignment, and Provider B for the second assignment. If Provider C was not available, the County would contact Provider D and Provider C would move to the bottom of the list, placing Provider E next in the rotation. If Provider B has skills that the other providers do not have, and the County requires the skills of Provider B for an assignment, the County may make an assignment out of order to Provider B even if Provider B was not up next in the rotation.
5. Pre-Approved Form Contract — Applicants will be required to execute a contract with the County using the Pre-Approved Form Contract (the Form Contract), including the General Conditions of Contract Between the County and Contractor ("General Conditions"), without modification.
6. Cost — The cost of contracts will not exceed available appropriations. Funds will be encumbered under a contract specifically for the services to be provided under the Contract(s) resulting from this Open Solicitation.
7. Cancellation — The County reserves the option to cancel this Open Solicitation at any time.
8. Award of a Contract under this Open Solicitation is subject to fiscal appropriations.
9. Changes to Forms – At the request of the Office of Procurement, the County may update the Open Solicitation Form contract with updated versions of the forms listed below without issuing an amendment to the Open Solicitation or to existing contracts:
   a. General Conditions of Contract Between County & Contractor (PMMD-45);
   b. Minority Business program & Offeror's Representation (PMMD-90);
   c. Montgomery County MFD Report of Payments Received (PMMD-97);
   d. Minority-owned Business Addendum to the General Conditions of Contract between County and Contractor (PMMD-91);
   e. Minority, Female, Disabled (MFD) Person Subcontractor Performance Plan. (PMMD-65); and
   f. Wage Requirements for Services Contract Addendum to The General Conditions of Contract Between County and Contractor (PMMD-177).

OPEN SOLICITATION #1161701
Animal Behaviorist Services

NOTICE TO VENDORS

Montgomery County, Maryland (the "County"), through its Office of Animal Services (OAS) seeks applications from qualified vendors to provide onsite animal behaviorist services. OAS serves and protects all animals and citizens in Montgomery County with dedication and compassion. The goal of the OAS is to strengthen the human-animal bond through education, humane law enforcement, and by promoting responsible guardianship.

Montgomery County intends to enter into multiple contracts resulting from this solicitation.

Compensation for services rendered under a Contract resulting from this Open Solicitation will be paid at the following fully burdened rate of $26.00 per hour.

Under no circumstances will the payment exceed the above established rates. The County reserves the option to cancel this Open Solicitation at any time.

Award of a Contract under this Open Solicitation is subject to fiscal appropriations. The County's fiscal year starts on July 1 and ends on the following June 30. Compensation for services rendered under a Contract resulting from this Open Solicitation will be paid at the current rates noted above for Montgomery County Fiscal Year 24 (July 1, 2023, through June 30, 2024).

The established rates will be in effect for each County fiscal year to start on July 1 and end on the following June 30. Under no circumstances will the payment exceed the established rates. The County may update Attachments E through I as needed, prior to Contractor's signature.

Established rates may be changed at the County's discretion at the beginning of each fiscal year, the County makes no guarantee that it will change fees at any point during the term of the contracts resulting from this Open Solicitation. Notification of rate changes will be posted prior to the start of the County's new fiscal year on July 1st. Rates will be posted to the following site: http://www.montgomerycountymd.gov/pol/chief/bureaus/management/mgmtbudget/InformalSolicitations.html

If this site changes the County will issue an Addendum to this Open Solicitation which will specify the updated site where the current rates are posted.

All applicants meeting the minimum qualifications listed in the Pre-Approved Form Contract of this Open Solicitation will be awarded a contract for services, however, this does not guarantee that any Contractor will receive a minimum amount of work.

All Contractors being awarded a contract must maintain the insurance limits set forth in the Form Contract at all times during the term of the Contract regardless of the amount of business received from the Contract.

OPEN SOLICITATION #1161701

Animal Behaviorists

INSTRUCTIONS TO VENDORS

The County will enter into a contract with all applicants who meet the minimum qualifications as stated in Article III, Minimum Qualifications of the Pre-Approved Form Contract and are found to be a responsible organization and/or individual. The County will execute the contract and return a copy to the applicant. The executed Pre-Approved Form Contract with all Attachments will constitute the entire Contract. Please keep a copy of all these documents for your records. The applicant must sign the County's Pre-Approved Form Contract which includes the General Conditions of Contract Between County and Contractor and other Attachments, as written with no modification.

Please direct Technical Questions to Thomas Koenig at 240-773-5225.
Please direct Application, Contract & Insurance Questions to Bonnie White at 240-372-7366.

I. SUBMISSION OF DOCUMENTS

All the following items must be submitted, or the application will be rejected:

1. Form Contract and Contract Attachments - the Form Contract must be filled out correctly and submitted along with the Attachments. *Please follow these steps:*
   A. Sign the Form Contract — If the applicant is a corporation, an officer of the corporation with authority to sign contracts for the corporation must sign the Form Contract.
   B. Enter a date only in the Signature Block. Please do not put a date in the paragraph at the top of the page.
   C. Submit all the pages of the Form Contract (not just the signature page) along with the General Conditions of Contract Between County & Contractor, (Attachment A); and the following attachments which must be completed in their entirety:
      - Attachment B, Application Form
      - Attachment C, "Minority, Female Disabled (MFD) Person Subcontractor Performance Plan" – this form must be filled out as much as possible. Please complete top section, A-F, sign and date. A full waiver may be requested; follow F & G.
      - Attachment D, "Wage Requirements for Services Contract Addendum to The General Conditions of Contract Between County and Contractor".
      - Attachment E, "Minority Business program & Offeror's Representation" — this form may be filled out and submitted if applicable to the applicant's organization.
      - Attachment F- County Administrative Procedures 6-1 and 6-7.
      - Attachment G-1, Independent Contractor Acknowledgement, Attachment G-2, Contactor Employee Acknowledgement.
2. A list of qualifications and related experience. Animal behaviorist services require two years of related experience.
3. Certificate of Insurance that provides evidence of meeting the Mandatory Insurance Requirements set forth in Article VI of the Pre-Approved Form Contract. Contact your insurance broker to obtain the Certificate.
4. Proof of Legal Name
   A. Articles of Incorporation, and Articles of Amendment (if applicable).
   B. W-9 Form or copy of Social Security card if Sole Proprietorship.
5. Proof of Tax-Exempt Status - IRS Determination Letter (if applicable).

II. INSTRUCTIONS

As directed above in Section I., please complete, attach, and send all Submission Documents to:

Montgomery County, Maryland
Office of Animal Services
Attn: Bonnie White
7315 Muncaster Mill Road
Derwood, MD 20855

If your application meets the minimum qualifications listed in the Pre-Approved Form Contract, the County will execute the contract and return a copy to you.

A copy of the County's General Conditions of Contract Between County and Contractor ("General Conditions") is included with the solicitation packet. The County's General Conditions will be attached as Attachment A to any contract that results from this Open Solicitation and includes terms and conditions that the County requires of Contractors. You must sign the County Pre-Approved Form Contract as written, and return it, with all attachments, to the County for execution by the Office of Procurement. The Office of Animal Services Contract Team will forward a copy of the executed contract to you.

No services may be provided until you receive notice from the County that the contract has been executed and receive an executed purchase order and request for services from the County.

The County makes no guarantee that any single contractor will receive a request to provide services under a contract resulting from this Open Solicitation. Work assignments will be made on a rotating basis in the order in which the contracts are executed, unless a unique skill set is required, in which case the County may contact the provider with the unique skills required for a particular assignment, even if that provider is not up next in the rotation. For example, if five contracts are executed because of this Open Solicitation, the County would contact Provider A for the first assignment, and Provider B for the second assignment. If Provider C was not available, the County would contact Provider D and Provider C would move to the bottom of the list, placing Provider E next in the rotation. If Provider B has skills that the other providers do not have, and the County requires the skills of Provider B for an assignment, the County may make an assignment out of order to Provider B even if Provider B was not up next in the rotation.

Award of a contract under this Open Solicitation is subject to fiscal appropriations. The County reserves the right to cancel this Open Solicitation at any time. Compensation for services rendered under a Contract resulting from this Open Solicitation will be paid at the current rates noted above for Montgomery County Fiscal Year 24 (July 1, 2023, through June 30, 2024) noted in the Notice to Vendors for Animal Behaviorists for Open Solicitation #1161701.

The established rates will be in effect for each County fiscal year to start on July 1 and end on the following June 30. Under no circumstances will the payment exceed the established rates. Established rates may be changed at the County's discretion at the beginning of each fiscal year, the County makes no guarantee that it will change fees at any point during the term of the contracts resulting from this Open Solicitation. Notification of rate changes will be posted prior to the start of the County's new fiscal year on July 1st. Rates will be posted to the following site:

http://www.montgomerycountymd.gov/pol/chief/bureaus/management/mgmtbudget/InformalSolicitations.html

If this site changes the County will issue an Addendum to this Open Solicitation which will specify the updated site where the current rates are posted.

OPEN SOLICITATION #1161701
ATTACHMENT B

APPLICATION FORM

CONTRACTOR LEGAL NAME:____

ADDRESS: ____

TELEPHONE: ____

EMAIL: ____

NAME AND TITLE OF MAIN CONTACT PERSON: ________________________________

I ACKNOWLDEDGE RECEIVING, READING, UNDERSTANDING AND AGREEING TO PERFORM THE SERVICES AS DELINEATED IN THE SOLICITATION PACKAGE AND THE FORM CONTRACT, UNDERSTAND THE REQUIREMENTS OF THIS SOLICITATION AND ACCEPT THE FEE SCHEDULE FOR SERVICES.

THE ENTITY APPLYING FOR A CONTRACT UNDER THIS SOLICITATION HAS THE CAPACITY, STAFF, QUALIFICATIONS LICENSING FINANCIAL STABILITY AND EXPERIENCE TO PERFORM SERVICES AS REQUIRED.

SIGNATURE: ______________________________ DATE: ________________

PRINTED: ______________________________

TITLE: ______________________________

OPEN SOLICITATION #1161701
Contract #____________

The County seeks to solicit proposals from and to enter into multiple contracts with qualified entities who can provide onsite animal behaviorist services for animals housed at the Montgomery County Animal Services and Adoption Center located at 7315 Muncaster Mill Road, Derwood, Maryland 20855.

I. SCOPE OF SERVICES

1. Perform behavioral assessments on shelter animals and reporting findings of behavioral assessments through oral and written communication.
2. Communicate effectively with Animal Services and Adoption Center staff regarding any concerns or adoption/rescue recommendations.
3. Conduct periodic checks of all shelter animals to assess suitability for play groups; criteria to include mandatory stray holding periods, behavior and medical considerations.
4. Assist and participate in efforts to enrich, socialize and exercise shelter animals.
5. Assist residents, as needed, interested in adopting shelter animals.
6. Provide counseling to residents, as needed, who may be looking to surrender a pet.
7. Respond to questions about specific animals and their behaviors.
8. Document and report any behavior abnormalities of shelter animals.
9. Notify the Shelter Operations Manager, Veterinary staff or Animal Care Attendant Supervisors of any significant observations and update the County's Chameleon system with results of observations.
10. Follow proper cleaning and sanitation procedures for play yards and evaluation rooms.
11. Hours of Service: Typical hours will fall between 7 a.m., and 7 p.m., 5 days-a-week including Saturdays and Sundays, on occasion these hours may be adjusted to cover specific tasks or activities.

County Responsibility

The County will monitor and review the work being performed by each Contractor under this Contract.

II. COMPENSATION

1. The County will compensate, and the Contractor agrees to invoice the County for services Provided under this Contract at the following fully burdened hourly rate of $26.00 per hour.
2. Under no circumstances will the payment exceed the established rates. Established rates may be changed at the County's discretion at the beginning of each fiscal year, the County makes no guarantee that it will change fees at any point during the term of the contracts resulting from this Open Solicitation. Notification of rate changes will be posted prior to the start of the County's new fiscal year on July 1st. Rates will be posted to the following site: http://www.montgomervcountvmd.gov/polichieMbureausimanagement/mgmtbudget/InformalSoli citations.html.
3. If this site changes the County will issue an Addendum to this Open Solicitation which will specify the updated site where the current rates are posted.
4. No services will be performed or compensated under this Contract without the Contractor's receipt of a County purchase order for a specific period during which services will be performed and containing a maximum amount of compensation.
5. The Contractor will invoice and be compensated for no more than the rates specified above.

III. MINIMUM QUALFICATIONS

The Contractor must ensure that any personnel providing services under this Contract meets the following minimum qualifications during all terms of this Contract:

1. Two (2) years of experience in an animal shelter or rescue organization or other work environment focused on the needs, care and behavior of animals.
2. Knowledge in the proper care and feeding of animals and be able to identify behavior tendencies in animals related to a variety of circumstances both physical (age, gender, breed, etc.) and otherwise.
3. Knowledge of animal behavior patterns and the ability to identify these patters particularly about animals that have been abused, mistreated, abandoned, or otherwise expose to harsh or traumatic circumstances.
4. Three (3) years of experience working with companion animal behavior and assessment in an applicable animal service setting. Preference for CPDT-KA certification or similar.
5. An equivalent combination of education and experience may be substituted.
6. Preference will be given to applicants who can demonstrate experience in performing behavioral assessments on shelter animals; report findings of behavioral assessments through oral and written communication; communicate issues or concerns related to the adoptability or transfer of an animal; assess suitability for an animals inclusion into play groups; develop enrichment programs for shelter animals; document and report any behavior abnormalities of shelter animals; follow proper cleaning and sanitation procedures; and/or update computer databases regarding observations.
7. The Contractor must accept the County established rates for services described in Open Solicitation #1161701 and as set forth in the County's currently defined rates in Article II. Compensation, Paragraph A of this Contract.
8. The Contractor must include a certificate of good standing with the Maryland State Department of Assessments & Taxation (SDAT), when applicable. SDAT may not be applicable for individuals, sole proprietorships, or partnerships.
9. The Contractor must comply with the County’s mandatory insurance requirements as set forth under Article VI of this Contract and must provide insurance certificate(s) evidencing the required insurance coverage which must remain in force without lapse during all terms of this Contract, regardless of contracted boarding fees paid to the Contractor. Even if a Contractor does not receive any boarding requests from the County it must continue to carry insurance coverage in the amounts designated in the MANDATORY MINIMUM INSURANCE REQUIREMENTS section of this Contract.

IV. INVOICES

The Contractor must submit monthly invoices and supporting documentation in a format approved by the County no later than 15 days following the end of each month. The Contractor must include, at a minimum, on each invoice, the Contractor's name, address, contract number, purchase order number, the hours and services provided, the date(s) the services were provided and the amount that is due based on the hourly rates set forth in this Contract. Upon receipt, acceptance and approval of the Contractor's invoice, the County will make payment, within 30 days, at the rates specified in Article II, Compensation. All required reports and other supporting documentation must be provided with the Contractor's monthly invoice. Invoices must be sent to the Program Manager designated by the County.

V. TERM

This Contract is effective upon signature by the County's Director, Office of Procurement, and is for a two-year term. Before the contract term ends, and subject to fiscal appropriations, 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. Contractor's satisfactory performance does not guarantee renewal of this Contract. The Director may exercise this option to renew for two (2) additional two-year terms.

VI. GENERAL CONDITIONS AND INSURANCE

The attached General Conditions of Contract Between County and Contractor are incorporated by reference and made a part of this Contract as Attachment A. Prior to the execution of the contract by the County, the Contractor must obtain at their own cost and expense the following insurance with an insurance company/companies license to do business in the State of Maryland.

The following minimum insurance requirements supersede those outlined in Provision #21 of the General Conditions.

(REMAINDER OF PAGE INTENTIONALLY LEFT BLANK)

MANDATORY MINIMUM INSURANCE REQUIREMENTS – Animal behaviorist services

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 ***one million dollars ($1,000,000), 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

Worker's Compensation/Employer's Liability – can be waived if contractor is a sole proprietor
Meeting all statutory requirements of the State of Maryland Law and with the following minimum Employers' Liability limits:

Bodily Injury by Accident - $100,000 each accident
Bodily Injury by Disease - $500,000 policy limits
Bodily Injury by Disease - $100,000 each employee

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 cancelled before the expiration date thereof, written notice must be delivered to the County in accordance with the policy provisions.

Certificate Holder
Montgomery County, Maryland
Montgomery County Police / Bonnie White
7315 Muncaster Mill Rd
Derwood, MD 20855

VII. COMPUTER RESOURCES SECURITY

The Contractor may be afforded remote access privileges to County Information Resources, or otherwise work on, or interface with, County Information Resources, and must 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). The Contractor must adhere to any and all policies and procedures under, or related to, the County's Information Resources Security Procedure (AP 6-7), which is expressly attached to this Contract as Attachment F incorporated by reference into, and made a part of this Contract as Attachment F.

The County's Information Resources Security Procedure (AP 6-7) references the County Computer Security Guideline and the County's Administrative Procedure 6-1. The County Computer Security Guideline (September 2010 version) and Administrative Procedure 6-1 are included in Attachment F, incorporated by reference into, and made a part of this contract.

VIII. INDEPENDENT CONTRACTOR/CONTRACTOR CONDUCT

1. For the purposes of this Contract, the Contractor's personnel engaged by the Contractor to perform services under this Contract are the employees, consultants, and workers of the Contractor. The Contractor's personnel are not employees of Montgomery County. The Contractor's personnel 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 may be mistaken for a County employee, the Contractor's personnel 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.
2. The Contractor must provide administrative oversight for and coordinate the recruitment, hiring/subcontracting, termination and placement of, qualified individuals who will provide services, including professional services upon the request of the County, as stipulated in this Contract for animal behaviorist and animal adoption counseling services. The Contractor must also provide overall supervision, control over, and direction of all personnel who work under this Contract in the provision of animal behaviorist and animal adoption counseling services.
3. 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 he employees, consultants, contractors, or other worker retained by the Contractor to provide services under this Contract.
4. The Contractor 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 worker's compensation for persons who work for the Contractor under this Contract.
5. The Contractor's personnel in the provision of providing the services under this Contract are not entitled to the use of, and must not use, County vehicles.
6. The Contractor's personnel 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 County employee benefits.

7. The Contractor, is solely responsible for all costs or expenses related to personnel costs of its personnel, including those related to wages, benefits, training, mileage, travel, parking, fringe benefits and paid leave.
8. 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, including, but not limited to pamphlets, surveys, evaluations, training materials and customized software. Any materials, records, or reports produced by the Contractor's personnel performing work under this Contract e are the County's property.
9. The County will own all work products produced 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 will have no such rights to work products produced for the County.
10. The Contractor must ensure that all personnel assigned to the County (to provide services under this Contract have provided a signed and witnessed copy of the following documents, as appropriate as determined by their status with the Contractor or subcontractor: 1) Attachment G-1— Independent Contractor Acknowledgement; and 2) Attachment G-2 — Contractor Employee Acknowledgement.

(REMAINDER OF PAGE INTENTIONALLY LEFT BLANK)

IX. PRIORITY OF DOCUMENTS

1. This **Contract** document;
2. The **General Conditions** of Contract Between County and Contractor **(Attachment A);**
3. The Open Solicitation **Application** Form **(Attachment B);**
4. Minority, Female Disabled **(MFD)** Person Subcontractor Performance Plan **(Attachment C);**
5. **Wage Requirements** for Services Contract **(Attachment D),** "Wage Requirements for Services Contract Addendum to The General Conditions of Contract Between County and Contractor: and
6. Minority Business Program & Offeror's Representation — this form may be filled out and submitted if applicable to the applicant's organization **(Attachment E);**
7. Administrative Procedures 6-1 and 6-7 **(Attachment F);** and
8. Independent Contractor Acknowledgement **(Attachment G-1)** and Contractor Employee Acknowledgement **(Attachment G-2).**

[SIGNATURE PAGE FOLLOWS]

OPEN SOLICITATION #1161701
Contract #_______

SIGNATURE PAGE

This Contract, which incorporates by reference: The Instructions to Vendors, the Notice to Vendors, the Approved Form Contract with attached General Conditions of Contract Between County and Contractor, Attachment A through G-2, the completed Application Form, copies of which have been provided to the Contractor, is entered into this day of ___, ___________ 2023 by and between (the "Contractor") and Montgomery County, Maryland (the "County"). This Contract will become effective on the date of signature by the Director, Office of Procurement. This Contract and any renewals or extensions of this Contract are subject to the appropriation of funds.

Part A: Contractor's Offer to Provide Services

(Prospective Contractor Must Complete The Below)

Name of Contracting Corporation, Partnership, Limited Liability Company, or Proprietorship

Signature*

Typed Name

Title

Date

Part B: County Acceptance

MONTGOMERY COUNTY, MARYLAND

Avinash Shetty, Director
Office of Procurement

Date

RECOMMENDED:

Thomas J. Koenig, Executive Director
Office of Animal Services

*Must be signed by corporate officer or person legally authorized to bind organization to a contract

THE OFFICE OF COUNTY ATTORNEY HAS APPROVED THIS FORM AS TO FORM AND LEGALITY.

ATTACHMENT A

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.

B. 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.

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

D. 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.

E. 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
Disease (policy limits)	500	500	500	Attachment

Disease (each employee)	100	100	100	
Commercial General Liability for bodily injury and property damage per occurrence, including contractual liability, premises and operations, and independent contractors	300 Attachment	500	1,000	See
Minimum Automobile Liability (including owned, hired and non owned automobiles)				
Bodily Injury				
each person	100	250	500	See
each occurrence	300	500	1,000	Attachment
Property Damage				
each occurrence	300	300	300	
Professional Liability* for errors, omissions and negligent acts, per claim and aggregate, with one year discovery period and maximum deductible of $25,000	250	500	1,000	See Attachment

Certificate Holder
Montgomery County Maryland (Contract #)
Office of Procurement
27 Courthouse Square, Ste 330
Rockville, Maryland 20850

*Professional services contracts only

(Remainder of Page Intentionally Left Blank)

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

	Up to 50	Up to 100	Up to 1,000	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, Ste 330
Rockville, Maryland 20850

(Remainder of Page Intentionally Left Blank)

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.

ATTACHMENT C

MONTGOMERY COUNTY, MARYLAND

MINORITY, FEMALE, DISABLED PERSON SUBCONTRACTOR PERFORMANCE PLAN

Contractor's Name: ______________________________

Address: ______________________________

City: ____________________ State: __________ Zip: __________

Phone Number: __________ Fax Number: __________ Email: ______________

CONTRACT NUMBER/PROJECT DESCRIPTION: ______________________________

A. Individual assigned by Contractor to ensure Contractor's compliance with MFD Subcontractor Performance Plan:

Name: ______________________________

Title: ______________________________

Address: ______________________________

City: ____________________ State: __________ Zip: __________

Phone Number: __________ Fax Number: __________ Email: ______________

B. This Plan covers the life of the contract from contract execution through the final contract expiration date.

C. The percentage of total contract dollars, including modifications and renewals, to be paid to all certified minority owned business subcontractors, is ________% of the total dollars awarded to Contractor.

D. Each of the following certified minority owned businesses will be paid the percentage of total contract dollars indicated below as a subcontractor under the contract.

I hereby certify that the business(s) listed below are certified by one of the following: Maryland Department of Transportation (MDOT); Federal SBA (8A); MD/DC Minority Supplier Development Council (MSDC); Women's Business Enterprise National Council (WBENC); or City of Baltimore. A Certification Letter must be attached. For assistance, call 240-777-9912.

1. Certified by: ______________________________

Subcontractor Name: ______________________________

Title: ______________________________

Address: ______________________________

City: ____________________ State: __________ Zip: __________

Phone Number: __________ Fax Number: __________ Email: ______________

CONTACT PERSON: ______________________________

Circle MFD Type:

AFRICAN AMERICAN   ASIAN AMERICAN   DISABLED PERSON
FEMALE   HISPANIC AMERICAN   NATIVE AMERICAN

The percentage of total contract dollars to be paid to this subcontractor : ______________________

This subcontractor will provide the following goods and/or services: ______________________

2. Certified by: ______________________

Subcontractor Name: ______________________

Title: ______________________

Address: ______________________

City: ______________________ State: Zip:

Phone Number: __________ Fax Number: __________ Email: __________

CONTACT PERSON: ______________________

Circle MFD Type:

AFRICAN AMERICAN ASIAN AMERICAN DISABLED PERSON
FEMALE HISPANIC AMERICAN NATIVE AMERICAN

The percentage of total contract dollars to be paid to this subcontractor: ______________________

This subcontractor will provide the following goods and/or services: ______________________

3. Certified by: ______________________

Subcontractor Name: ______________________

Title: ______________________

Address: ______________________

City: ______________________ State: __________ Zip: __________

Phone Number: __________ Fax Number: __________ Email: __________

CONTACT PERSON: ______________________

Circle MFD Type:

AFRICAN AMERICAN ASIAN AMERICAN DISABLED PERSON
FEMALE HISPANIC AMERICAN NATIVE AMERICAN

The percentage of total contract dollars to be paid to this subcontractor: ______________________

This subcontractor will provide the following goods and/or services: ______________________

4. Certified By: ______________________

Subcontractor Name: ______________________________

Title: ______________________________

Address: ______________________________

City: ____________________ State: __________ Zip: __________

Phone Number: __________ Fax Number: __________ Email: ______________

CONTACT PERSON: ______________________________

Circle MFD Type:

AFRICAN AMERICAN ASIAN AMERICAN DISABLED PERSON
FEMALE HISPANIC AMERICAN NATIVE AMERICAN

The percentage of total contract dollars to be paid to this subcontractor: ______________________

This subcontractor will provide the following goods and/or services: ______________________

____

E. The following language will be inserted in each subcontract with a certified minority owned business listed in D above, regarding the use of binding arbitration with a neutral arbitrator to resolve disputes with the minority owned business subcontractor; the language must describe how the costs of dispute resolution will be apportioned:

____

____

____

____

F. Provide a statement below, or on a separate sheet, that summarizes maximum good faith efforts achieved, and/or the intent to increase minority participation throughout the life of the contract or the basis for a full waiver request.

____

____

____

____

____

G. A full waiver request must be justified and attached.

Full Waiver Approved:

____________________ Date: __________

MFD Program Officer

Partial Waiver Approved:

____________________ Date: __________

MFD Program Officer

Full Waiver Approved:

____________________ Date: __________

Avinash Shetty
Director
Office of Procurement

Partial Waiver Approved:

____________________ Date: __________

Avinash Shetty
Director
Office of Procurement

The Contractor submits this MFD Subcontractor Performance Plan (Plan Modification No.) in accordance with the Minority Owned Business Addendum to General Conditions of Contract between County and Contractor.

CONTRACTOR SIGNATURE

USE ONE:

1. TYPE CONTRACTOR'S NAME: ______________________________

____
Signature

____
Typed Name

____
Date

2. TYPE CORPORATE CONTRACTOR'S NAME: ______________________________

____
Signature

____
Typed Name

____
Date

I hereby affirm that the above-named person is a corporate officer or a designee empowered to sign contractual agreements for the corporation.

____
Signature

____
Typed Name

____
Title

____
Date

APPROVED:

______________________________ ______________________________
Avinash Shetty, Director, Office of Procurement Date

Section 7.3.3.4(a) of the Procurement Regulations requires:
The Contractor must notify the Director, Office of Procurement of any proposed change to the Subcontractor Performance Plan.

ATTACHMENT D

Requirements for Services Contract
Addendum to The General Conditions of Contract Between County and Contractor

A. This contract is subject to the Wage Requirements Law, found at Section 11B-33A of the Montgomery County Code ("WRL" or "11B-33A"). A County contract for the procurement of services must require the contractor and any of its subcontractors to comply with the WRL, subject to the exceptions for particular contractors noted in 11B-33A (b) and for particular employees noted in 11B-33A (f).

B. Conflicting requirements (11B-33A (h)): If any federal, state, or County law or regulation requires payment of a higher wage, that law or regulation controls. For an existing County Contract, if an applicable collective bargaining agreement (CBA) that existed prior to May 10, 2016, governs the parties, then that CBA controls. If the term of the CBA mentioned in the preceding sentence ends during the Contract, the WRL will then control.

C. A nonprofit organization that is exempt from the WRL under 11B-33A (b)(3), must specify, in each bid or proposal, the wage the organization intends to pay to those employees who will perform direct, measurable work under the contract, and any health insurance coverage the organization intends to provide to those employees. Section 11B-33A (c)(2).

D. A contractor must not split or subdivide a contract, pay an employee through a third party, or treat an employee as a subcontractor or independent contractor, to avoid the imposition of any requirement in 11B-33A. Section 11B-33A (c)(3).

E. Each contractor and subcontractor covered under the WRL must: certify that it is aware of and will comply with the applicable wage requirements; keep and submit any records necessary to show compliance; and conspicuously post notices approved and/or supplied by the County, informing employees of the requirements in 11B-33A. Section 11B-33A (i).

F. An employer must comply with the WRL during the initial term of the contract and all subsequent renewal periods, and must pay the adjusted wage rate increase required under 11B-33A (e)(2), if any, which is effective July 1 of each year. The County will adjust the wage rate by the annual average increase in the Consumer Price Index for all urban consumers for the Washington-Baltimore metropolitan area, or successor index, for the previous calendar year and must calculate the adjustment to the nearest multiple of 5 cents. Section 11B-33A (e)(2).

G. An employer must not discharge or otherwise retaliate against an employee for asserting any right, or filing a complaint of a violation, under the WRL. Section 11B-33A (i)(3).

H. The sanctions under Section 11B-33 (b), which apply to noncompliance with nondiscrimination requirements, apply with equal force and scope to noncompliance with the wage requirements of the WRL. Section 11B-33A (i)(4).

I In the event of a breach of this contract as a result of a contractor's or subcontractor's violation of the WRL, the County may seek its available remedies, which include but are not limited to liquidated damages, withholding of payment, and recoupment of audit costs that are described below. The Contractor is jointly and severally liable for any noncompliance by a subcontractor. An aggrieved employee, as a third-party beneficiary, may, by civil action against the violating Contractor or subcontractor, enforce the payment of wages due under the WRL and recover from the Contractor or subcontractor any unpaid wages with interest, a reasonable attorney's fee, and damages for any retaliation by the Contractor or subcontractor arising from the employee asserting any right, including filing a complaint under the WRL. Section 11B-33A (i)(5). Furthermore, the contractor expressly acknowledges that the County may assess liquidated damages against the Contractor in the event that it, as a covered employer, fails to pay the required wage, or violates the wage reporting or payroll records reporting requirement found at 11B-33A (g), including providing late or inaccurate payroll records.

(i) Liquidated Damages

The County may assess liquidated damages for any noncompliance by contractor or its subcontractor at the rate of 1% per day of the total contract amount, or the estimated annual contract value of a requirements contract, for each day of the violation. This liquidated damages amount in addition to the amount of any unpaid wages, with interest. The Contractor must pay to the County liquidated damages noted above, in addition to any other remedies available to the County. Contractor and County acknowledge that damages that would result to the County as a result of a breach under the WRL are difficult to reasonably ascertain, and that the liquidated damages provided for in this paragraph is a fair and reasonable estimate of damages the County would incur as a result of contractor's or subcontractor's violation of the WRL.

(ii) Withholding of Payment

If the Director determines that a provision of the WRL has been violated, the Director must issue a written decision, including imposing appropriate sanctions and assessing liquidated damages (as outlined above) and audit costs (as outlined below), and may withhold from payment due the contractor, pending a final decision, an amount sufficient to: (a) pay each employee of the contractor or subcontractor the full amount of wages due under the WRL; (b) reimburse the County for audit costs; and (c) satisfy a liability of a contractor or subcontractor for liquidated damages.

(iii) Audit Costs

If the County determines, as a result of a WRL audit, that the Contractor has violated requirements of the WRL, the Contractor must reimburse to the County the cost incurred by the County in conducting the audit. Section 11B-33A (i)(2)(C).

J. The County must conduct, and the contractor or subcontractor must comply with, random or regular audits to assure compliance with the WRL. Section 11B-33A (i)(2). The Director may conduct an on-site inspection(s) for the purpose of determining compliance. Some of the documents that may be required during an audit are listed on the Wage Requirements Law FAQ web page: https://www.montgomerycountymd.gov/PRO/DBRC/wage-requirements-law.html

K. The Contractor is in breach of this Contract if the Contractor fails to submit timely documentation demonstrating compliance with the WRL to the satisfaction of the Director, including: the Wage Requirements Law Payroll Report Form (PMMD-183), which is required to be submitted by the 14th day of the month following the end of each quarter (January, April, July, October); documents requested in conjunction with a random or regular audit by the County; or, documents otherwise requested by the Director. Section 11B-33A (g)(2).

If a contractor or subcontractor fails to submit, or is late in submitting, copies of any payroll record or other report required to be submitted under the WRL, the County may deem invoices unacceptable until the contractor or subcontractor provides the required records or reports, and may postpone processing payments due under the contract or under an agreement to finance the contract.

For any questions, please contact the Wage Requirements Law Program Manager at 240-777-9918 or WRL@montgomerycountymd.gov.

Wage Requirements Law Certification

(Montgomery County Code, Section 11B-33A)

Business Name					
Address					
City		State		Zip Code	
Phone Number		Fax Number			
E-Mail Address					

Provide, in the spaces below, the contact name and information of the individual designated by your firm to monitor your compliance with the County's Wage Requirements Law, unless exempt under Section 11B-33A (b) (see Section B. below):

Contact Name			Title	
Phone Number		Fax Number		
E-mail Address				

In the event that you, the "Offeror," are awarded the contract and become a Contractor, please check ☑ the box(es) below that apply, and leave all of the other boxes blank.

□ A. Wage Requirements Compliance

This Contractor, as a "covered employer", must comply with the requirements under Montgomery County Code Section 11B-33A, "Wage Requirements" ("Wage Requirements Law" or "WRL"). Contractor and its subcontractors must pay all employees not exempt under the WRL, and who perform direct measurable work for the County, the required gross wage rate effective at the time the work is performed. For employees who are not paid an hourly wage, Contractor's compliance with the WRL must be measured by dividing the amount paid to the employee each pay period by the number of hours worked by that employee during each pay period. A covered employer must not make any deduction for any item necessary for an employee to perform the essential job function unless the deduction is permitted by Executive Regulation. The offer price(s) submitted under this solicitation include(s) sufficient funds to meet the requirements of the WRL. A "covered employer" must submit, within 14 days after the end of each quarter (by the 14th of January, April, July, and October, for the quarter ending the preceding month), certified payroll records for each payroll period and for all employees of the contractor or a subcontractor performing services under the County contract governed by the WRL. The payroll records must contain a statement signed by the contractor or subcontractor certifying that the payroll records are correct and the wage rates paid are not less than those required by the WRL. These payroll records must include the following: name, address and telephone number of the contractor or subcontractor; the name and location of the job; and each employee's name, current home address, daily straight time and overtime hours, total straight time and overtime hours for the payroll period, rate of pay, fringe benefits by type and amount, gross wages, race and gender of the employee, and the employer and the employee share of any health insurance premium provided to the employee. The Contractor must ensure that **NO** Social Security number of any person, other than the last four digits, is included on the quarterly report. A sample, blank Payroll Report Form, for your use and completion, can be found at: https://www.montgomerycountymd.gov/PRO/DBRC/wage-requirements-law.html. The above must be submitted to the Division of Business Relations and Compliance, Attn: Wage Requirements Law Program Manager (preferably via email to WRL@montgomerycountymd.gov), Each Contractor must: keep payroll records covering work performed on a contract covered by the WRL for not less than 5 years after the work is completed; and, subject to reasonable notice, permit the County to inspect the payroll records at any reasonable time and as often as the County deems necessary. If the Contractor or subcontractor fails to submit, or is late in submitting, copies of any payroll record or other report required to be submitted under the WRL, the County may deem invoices unacceptable until the Contractor or subcontractor provides the required records or reports, and may postpone processing payments due under the contract or under an agreement to finance the contract. A violation of the WRL, including the late submission or non-submission of the information noted above, may result in action by the County, including: (a) withholding contract payments, reducing payment amounts, or otherwise assessing damages against Contractor, in an amount sufficient to: (i) pay each employee of the Contractor or subcontractor the full amount of wages due under the WRL; (ii) reimburse the County for audit costs; or (iii) satisfy a liability of a contractor or subcontractor for liquidated damages; (b) terminating the contract; or, (c) otherwise taking action to enforce the contract or the WRL. Violation of the WRL may also result in a finding of non-responsibility for a future contract, or may form the basis for debarment or suspension.

B. Exemption Status (if applicable)

This Contractor is exempt from Section 11B-33A, "Wage Requirements," because it is:

1. Reserved – [Intentionally left blank].

□ 2. a contractor who, at the time a contract is signed, has received less than $50,000 from the County in the most recent 12-month period, and will be entitled to receive less than $50,000 from the County under that contract in the next 12-month period. Section 11B-33A (b)(1).

□ 3. a public entity. Section 11B-33A (b)(2).

□ 4. a non-profit organization that has qualified for an exemption from federal income taxes under Section 501(c)(3) of the Internal Revenue Code. Section 11B-33A (b)(3) **(must also complete item C below).**

□ 5. an employer expressly precluded from complying with the WRL by the terms of any federal or state law, contract, or grant. Section 11B-33A (b)(7) (**must specify the law, or furnish a copy of the contract or grant**).

□ C. Nonprofit Wage & Health Information

This Contractor is a non-profit organization that is exempt from coverage under Section 11B-33A (b)(3). The contractor must provide proof of its 501(c)(3) status (i.e. Letter from the IRS). Accordingly, the contractor has completed the 501(c)(3) Non-profit Organization's Employee's Wage and Health Insurance Form which is attached. See Section11B-33A(c)(2). **(must also complete box B.4. above)**

□ D. Sole Proprietorship

Sole Proprietorships are subject to the WRL. In order to be excused from the posting and reporting requirements of the WRL, the individual who is the sole proprietor must sign the certifications below in order to attest to the fact that the Sole Proprietorship:

(1) is aware of, and will comply with, the WRL, as applicable;
(2) has no employee other than the sole proprietor; and
(3) will inform the Montgomery County Division of Business Relations and Compliance if the sole proprietor employs any worker other than the sole proprietor.

Note: A schedule C from the employer's federal tax return may be required for verification purposes.

E. Sub-Contractors

It is the prime contractor's responsibility to ensure all of its subcontractors adhere to the WRL. All subcontractors are required to submit quarterly payroll reports. It is the prime contractor's responsibility to collect these payroll reports and submit them to wrl@montgomerycountymd.gov on a quarterly basis.

□ I intend to use Sub-Contractors if I am awarded a contract as a result of this solicitation.

□ I do **NOT** intend to use Sub-Contractors if I am awarded a contract as a result of this solicitation. If at any time during the course of the contract I use Sub-Contractors, I understand that I am responsible for their quarterly payroll reporting.

F. Independent Contractors

□ I intend to use Independent Contractors if I am awarded a contract as a result of this solicitation.

If this box is checked, you must complete the Wage Requirements Law Independent Contractor Certification (PMMD193) in order for your bid/offer to be considered. It can be found at:
https://www.montgomerycountymd.gov/PRO/Resources/Files/SolForm/PMMD-193.pdf

□ I do **NOT** intend to use Independent Contractors if I am awarded a contract as a result of this solicitation. If at any time during the course of the contract I use Independent Contractors, I understand and agree that I must complete the Wage Requirements Law Independent Contractor Certification (PMMD193). See above link.

Contractor Certification

CONTRACTOR SIGNATURE: Contractor submits this certification form in accordance with Section 11B-33A of the Montgomery County Code. Contractor certifies that it, and any and all of its subcontractors that perform services under the resultant contract with the County, adhere to Section 11B-33A of the Montgomery County Code.

Authorized Signature		Title of Authorized Person	
Typed or Printed Name		Date	

501(c)(3) Nonprofit Organization’s Employee’s Wage and Health Insurance Form

Business Name					
Address					
City		State		Zip Code	
Phone Number		Fax Number		E-Mail	

Please provide below the employee labor category of all employee(s) who will perform direct measurable work under this contract, the hourly wage the organization pays for that employee labor category, and any health insurance the organization intends to provide for that employee labor category:

Employee Labor Category	Wage per Hour	Name of Health Insurance Provider(s) and Plan Name* (e.g. ABC Insurer, Inc. , HMO Medical and Dental)

* IF NO HEALTH INSURANCE PLAN IS PROVIDED PLEASE STATE “NONE”.

MINORITY BUSINESS PROGRAM & OFFEROR'S REPRESENTATION

It is the policy of the County to recruit actively, minority-owned businesses to provide goods and services to perform governmental functions pursuant to Section 11B-57 of the County Code. Minority-owned businesses are described in County law as Minority/Female/Disabled Person owned businesses (MFD). MFD businesses include certain non-profit entities organized to promote the interests of persons with a disability demonstrating (on a contract by contract basis) that at least 51% of the persons used by the non-profit entity to perform the services or manufacture the goods contracted for by the County, are persons with a disability. MFD firms also include those firms that are 51% owned, controlled and managed by one or more members of a socially or economically disadvantaged minority group, which include African Americans who are not of Hispanic origin, Hispanic Americans, Native Americans, Asian Americans, Women and Mentally or Physically Disabled Persons.

Section 7 - "Minority Contracting", Montgomery County Procurement Regulations specifies the procedure to be followed and will govern the evaluation of offers received pursuant to this solicitation. A copy of Section 7 of the Procurement Regulations is available upon request.

Prior to awarding contracts with a value of $50,000 or more, a prospective Contractor must demonstrate that a minimum percentage of the overall contract value as set by the County, will be subcontracted to certified MFD businesses. A decision as to whether the prospective Contractor has demonstrated a good faith effort to meet this subcontracting requirement will be made by the Director, Office of Procurement, or his/her designee, who may waive this requirement.

A sample of the MFD Report of payment Received is attached. This form is mailed to the MFD Subcontractor to complete for documentation of payment by the Prime Contractor. It is not to be completed by the Prime Contractor nor submitted with the MFD Subcontractor Performance Plan.

The Director, Office of Procurement, or his /her designee determines whether a waiver of MFD subcontracting would be appropriate, under Section 7.3.3.5 of the Procurement Regulations.

For further information regarding the MFD Business Program, please contact the MFD Program Manager, Division of Business Relations and Compliance at (240) 777-9912.

Offerors are encouraged (but not required) to complete the following:

I hereby represent that this is a Minority Business firm as indicated below (CIRCLE ONE):

AFRICAN AMERICAN	ASIAN AMERICAN	DISABLED PERSON
FEMALE	HISPANIC AMERICAN	NATIVE AMERICAN

Attach one of the following certification documents from: Maryland Department of Transportation (MDOT); Federal SBA 8(a); MD/DC Minority Supplier Development Council, Women's Business Enterprise National Council; Department of Veterans Affairs; or City of Baltimore.

ATTACHMENT G-1

INDEPENDENT CONTRACTOR ACKNOWLEDGMENT

CONTRACT # ______________________

I understand that I am an independent contractor of __________________, performing the services specified in Open Solicitation #1161701 developed pursuant to this Contract for the term specified in this Contract, under subcontract with ______________, and I am not an employee of Montgomery County for any purpose.

I understand that I may not represent myself as an employee of the County in any interaction with the public, other contractors, or County employees. I understand that I may not set policies for the County or independently interpret County policies. I understand that in situations where I may be mistaken for a County employee, I have an obligation to disclose that I am not a County employee, but that I am working for a County contractor.

I understand that failure to perform in accordance with the Contract may result in termination of my assignment to Montgomery County.

I understand that I will not have any Federal, State, or local tax, FICA or Medicare withheld from County payments to _____________. As an independent contractor of ____________, payment of all fringe benefits, Social Security, and Federal, State, or local taxes is my sole responsibility.

____
Signature

____
Name

____
Date

____
Witness (Prime Contractor)

ATTACHMENT G-2

CONTRACTOR EMPLOYEE ACKNOWLEDGMENT

CONTRACT # ________________________

I understand that I am an employee of ___________________, performing the services specified in the Open Solicitation #1161701 developed pursuant to this Contract for the term specified in this Contract, and I am not an employee of Montgomery County for any purpose. For example, I am not entitled to any rights of an employee of Montgomery County such as vacation and sick leave, retirement and health benefits, and merit system protections.

I understand that I may not represent myself as an employee of the County in any interaction with the public, other contractors, or County employees. I understand that I may not set policies for the County or independently interpret County policies. I understand that in situations where I may be mistaken for a County employee, I have an obligation to disclose that I am not a County employee, but that I am working for a County contractor.

I understand that failure to perform in accordance with the Contract may result in termination of my assignment to Montgomery County.

____
Signature

____
Name (Print)

____
Date

____
Witness (Prime Contractor)

ATTACHMENT F

	MONTGOMERY COUNTY ADMINISTRATIVE PROCEDURE **Offices of the County Executive • 101 Monroe Street • Rockville, Maryland 20850**	NO. 6-1 PAGE Page 1 of 8 DATE 6/30/23
TITLE Use of County-Provided Technology		CAO APPROVAL

1. PURPOSE & SCOPE

1.1 To establish an administrative procedure governing the use of County Technology (defined below) and connectivity to the County network in order to safeguard County assets and operations and reduce the risks and liabilities associated with improper use and connectivity. The County provides a network and maintains County Technology, such as email, intranet, and Internet access to Users (defined below) for the purpose of improving productivity, professional development, and the level of service to the people of our community.

1.2 This Administrative Procedure applies to all use of County Technology. This includes County Technology that uses third-party networks that is not paid for or provided by the County (i.e., a county-provided computer using public Wi-fi).

1.3 This Administrative Procedure does not apply to the use of technology that has not been paid for or provided by the County, that is also not connected to the County's network or third-party networks or applications paid for by the County (i.e., personal devices using networks not paid for by the County). This Administrative Procedure is also not intended to and does not apply to County Technology that is intended for public use.

1.4 Although this Administrative Procedure applies to County Technology as defined below, all Users are advised that the use of any personal devices including a mobile device for official County business will implicate that device in data retention, the Maryland Public Information Act (MPIA), and litigation discovery. If an employee uses a personal device for County work, and the County needs to retrieve any data on that device, the employee must produce the data, or alternatively, produce the device so that the County may extract the necessary data.

2. DEFINITIONS

2.1 Department of Technology and Enterprise Business Solutions (TEBS) – A department in the executive branch that is responsible for automated information systems and telecommunications technology, pursuant to County Code § 2-58D.

2.2 CIO - Chief Information Officer and TEBS Department Head.

2.3 County Technology – Any technology that is provided by or paid for by the County, such as automated information systems, telecommunications technology, hardware, firewalls, supervisory control and data acquisition (SCADA) devices, wireless access points, routers, software, Internet access, intranet access, broadband connectivity, virtual private network (VPN), email, text messaging, cloud services, or collaboration platforms, and any County-provided device such as a desktop, laptop, mobile phone, tablet, or server.

2.4 Personal Device – any device that is not paid for or provided by the County.

2.5 Personal Use – Activity that is conducted for purposes other than accomplishing official or otherwise authorized activity.

2.6 Users – Employees, contractors, volunteers, and all other individuals that receive access to County Technology.

2.7 User Content – Data or communications generated, viewed, transmitted, or stored on County Technology by a User. This includes without limitation emails, text messages, or chat messages sent via collaborative technology.

3. POLICY

3.1 The County provides Users access to County Technology for the efficient exchange of information and the completion of assigned responsibilities that are consistent with the County's purposes.

3.2 Users must use County Technology responsibly and professionally and must not use County Technology in a manner that violates any applicable Federal, State, or Montgomery County law, regulation, or policy, including those contained in the County's Administrative Procedures.

3.3 A User may use County Technology for Personal Use on only a limited, reasonable basis, and in accordance with this Administrative Procedure. However, Users must act reasonably to minimize Personal Use of County Technology. Personal use of County Technology by Users should mainly be during personal time (before and after work or during lunch time). Such use must be kept to a minimum, must not increase or create additional expense to the County, and must not disrupt the conduct of service or performance of a User's official County duties.

3.4 Use of County Technology by a User is consent to this Administrative Procedure, and to the County's access and monitoring, for legitimate business purposes (including a non-investigatory work-related search or investigatory search of suspected misfeasance), of any User Content. This includes consent for the County to view or remove any User Content that poses a threat to the security of County Technology, without any prior notice to the User. When accessing County Technology, all Users must review and accept any conditions indicated on any County logon banners that appear on County Technology.

3.5 Users and departments must not purchase or connect any device, application, hardware, equipment, or County Technology to the County Network without express authorization from TEBS. Departments may not purchase or contract with Internet, broadband, or cloud services without express authorization from TEBS. Departments may not connect Internet, broadband, or cloud services to the County Network without express authorization from TEBS.

3.6 Users may only use and access County Technology in compliance with Administrative Procedure 6-7 on Information Security.

3.7 Any employee who is in violation of this Administrative Procedure may be subject to disciplinary action, including dismissal, and other legal remedies available to the County, in accordance with applicable Federal, State, or Montgomery County laws and regulations, including Personnel and Ethics Laws, currently codified at Chapter 33 and Chapter 19A, respectively, of the County Code and Regulations, and applicable collective bargaining agreements, as amended.

3.8 Exemptions – Any deviations from this policy require a written exemption request, which must be submitted by the Using Department. 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. The Chief Administrative Office (CAO) or designee may grant exemptions related to recordings. The CIO may approve exemptions to this policy with the exception of prohibitions against recording and the allowance of reasonable Personal Use of County Technology.

4. PROHIBITED USER CONDUCT

4.1 Users must use County Technology in accordance with this Administrative Procedure and all applicable laws, regulations, and policies. Unless required for a User's documented job duties, prohibited User conduct, including Personal Use, includes:

4.1.1 Accessing, sending, forwarding, storing, or saving on County Technology any material that is offensive, demeaning or disruptive, including messages that are inconsistent with the County's policies concerning "Equal Employment Opportunity" and "Sexual Harassment and Other Unlawful Harassment," for any reason other than for purposes of eliminating this type of material from County systems. The act of inadvertently opening an email that contains this type of material does not, itself, constitute a violation of this policy;

4.1.2 Personal Use beyond that permitted by this policy;

4.1.3 Any use prohibited by Federal, State, or County law;

4.1.4 Users may not modify County Technology for personal purposes. This includes: loading of personal software or non-County supplied software; "shareware" and/or "freeware"; and animated (executable) screen savers or peer-to-peer software packages. Examples of inappropriate personal configuration include adding unauthorized wireless network cards, use of external storage devices that contain applications, and communications or video components not supplied or tested by the County;

4.1.5 Using County Technology to gain unauthorized access to County or other system resources;

4.1.6 Using County Technology to gamble, or other illegal or County-prohibited activities;

4.1.7 Using County Technology for private gain or profit;

4.1.8 Illegally copying material protected under copyright law or making that material available to others for copying. Users must comply with copyright law and applicable licenses that may apply to photographs, software, files, graphics, documents, messages, and other material Users wish to download or copy;

4.1.9 Using County Technology to publish or represent (expressly or implicitly) personal or unofficial opinions as those of the County;

4.1.10 Any Personal Use that could cause congestion, delay, or disruption of service to any County system or equipment. This may include, but not be limited to:

- "Chain" or unnecessary "Reply All" emails; and
- Downloads of video, sound, or other large, non-work-related files;

4.1.11 Sending broadcast messages to all, or the majority of, County Technology Users without obtaining prior approval from the CAO or their designee, in accordance with County information technology policies and procedures: and

4.1.12 Using non-TEBS authorized third-party communication systems and storage servers such as Google, Yahoo, and MSN Hotmail etc. to conduct Montgomery County business or to store or retain communications on behalf of the County. Such communications and transactions should be conducted through proper channels using County-approved procedures.

5. COUNTY OWNERSHIP, MONITORING, CONTROL, AND DISCLOSURE

5.1 All County Technology is the property of, or licensed to, the County.

5.2 Any data stored, created, transmitted, or received with County Technology is the property of the County and, therefore, is not considered private. This includes email from an employee's personal account if that email is stored or accessed on the County's computer resources.

5.3 Electronic files and messages created with County Technology may be accessed by the County without prior notice to a User, even if the User deleted the electronic files and messages. These electronic messages and files may also be used by the County in disciplinary or other proceedings.

5.4 Users must take appropriate measures to prevent unauthorized access to confidential information when using County Technology, in accordance with applicable Federal, State, or Montgomery County laws, regulations, or policies regarding confidential information.

5.5 The County may monitor a User's use of County Technology, and may access a User's Content when there is a legitimate business purpose (including a non-investigatory work-related search or investigatory search of suspected work-related misfeasance). This includes access to email messages from an employee's personal email account, if the personal email is stored in or accessed via County Technology. This applies to text messages that relate to County business as well.

5.6 Access to User Accounts for Investigatory or Business Purposes

5.6.1 The County Executive, the Chief Administrative Officer, Deputy or Assistant Chief Administrative Officer, or attorneys in the Office of the County Attorney may authorize in writing that a TEBS system administrator access a User's account (such as email, files, sites or other information). The access authority set forth in the prior sentence does not apply to the accounts of County Council and Legislative Office Users. Any of these individuals who authorize a TEBS system administrator to access a User's account should notify the affected User's department head of that access. Such notice is not required, however, if the basis for the access is of such a nature that department head notice would not be appropriate or legal, e.g., a confidential investigation or a non-public grand jury subpoena.

5.6.2 In addition to the above, a User's account may be accessed upon a written request from the User's department head with approval by the CIO or designee.

5.6.3 Access into a User's account pursuant to this Section 5.6 is appropriate only if there is a legitimate business purpose (including a non-investigatory work-related search or investigatory search of suspected work-related misfeasance) or legal need for such an action.

5.6.4 The existence of privately held passwords and "message delete" functions do not restrict or eliminate the County's ability or right to access User account information.

5.7 As part of its official duties and pursuant to County law, the Office of the Inspector General is authorized to access and receive a User’s emails or other files. The department head notice requirement in Section 5.6.1 does not apply to Office of the Inspector General.

5.8 In addition to the above, a User's email or other files may be accessed upon a written request from the User's department head with approval by the CIO or designee.

5.9 The County may monitor or control the flow of Internet, intranet, and email traffic over the County’s network for security or network management reasons, or for other legitimate business purposes.

5.10 The County has the right to utilize software to identify and block access to Internet sites containing sexually explicit or other material deemed inappropriate in the workplace.

5.11 The County may be compelled to access and disclose to third parties any electronic communications sent over County Technology in accordance with the Maryland Public Information Act (MPIA), Md. Code Ann., Gen. Prov. (“GP”) § 4-101 et seq. Electronic communications includes without limitation emails, texts, or chat messages sent via collaborative platforms or solutions. The MPIA applies to an electronically stored email message or a hard copy of the message in the custody and control of a public officer or employee, if the message is related to the conduct of public business. 81 Op. Att’y Gen, Op No. 96-016, 1996 WL 305985 (1996).

6. CREATING RECORDINGS OR TRANSCRIPTION WITH COUNTY TECHNOLOGY: PROHIBITED

6.1 Recording or transcription of meetings using County Technology is prohibited.

6.1.1 The prohibition against recording does not apply to the Office of the Inspector General, police body-worn cameras, criminal investigations, investigations related to County Code enforcement, and internal departmental investigations of suspected workplace misconduct or ethics violations.

6.2 Exceptions to the prohibition against recording or transcribing meetings for valid business purposes may be granted by the CAO, or designee, in writing, in response to a written request justifying the need to record the meeting. In general, only the following needs to record or transcribe will be approved:

6.2.1 Public meetings where there is no reasonable expectation of privacy and that are subject to the Open Meetings Act, such as legislative sessions.

6.2.2 High-impact, County-wide trainings that are of an enduring quality that are replayed frequently verbatim for a large group of employees, contractors, volunteers, or other individuals where there is no reasonable expectation of privacy. Trainings that are specific to only a small number of individuals within a department are not appropriate for recording or transcription.

6.3 If the technology being used to record the meeting or training has a “chat” or “comment” feature that allows public comment, it must be turned off during the meeting. Enabling the chat feature on a recorded meeting or training requires a specific exemption from the CAO or designee.

6.4 Even if a meeting or training has CAO or designee approval to record, it is never appropriate to record or transcribe a meeting that involves:

6.4.1 Legal advice from the Office of the County Attorney or any outside attorneys retained to represent the County;

6.4.2 Information that by law must be kept confidential and non-public, including without limitation Protected Health Information as defined by HIPAA, emergency plans or protocols, or non-public discussions that may be subject to Executive Privilege. Executive Privilege protects pre-decisional communications that precede a final decision on an issue.

6.5 Even if a meeting or training has CAO or designee approval to record, use of County Technology must comply with all applicable Federal, State, and County laws and policies.

6.5.1 Maryland law prohibits audio recording or transcribing of any participant to (1) an in-person oral communication spoken in private conversation or (2) a wire or electronic communication without their consent, with limited exceptions. Examples of wire or electronic communications include a telephone call or a communication that occurs over a collaborative service such as Microsoft Teams. Any use of County Technology that records those participants must ensure the consent of all participants.

6.5.2 One way to ensure consent is to communicate at the beginning of the meeting that the meeting is being recorded or transcribed and that continued participation represents the participant's consent to being recorded. Unless the technology being used to record automatically notifies individuals who join a meeting late, any individual that joins the meeting late must be notified that it is being recorded or transcribed and their continued presence represents consent to be recorded.

6.5.3 Any recording posted on the internet must comply with applicable accessibility laws.

6.6 The recording or transcription of electronic communications:

6.6.1 may only occur on platforms that are organizationally approved and managed by the County;

6.6.2 may only occur after participants have been notified and have either explicitly consented to the recording or have been permitted the opportunity to leave the call;

6.6.3 are the property of the County; and

6.6.4 may be subject to inspection, in part or in whole, as a public record.

6.7 Departments must maintain an index of all County-created recordings and transcriptions of trainings or meetings. Any individual who records or transcribes a meeting must notify their Department Records Coordinator so that the recording or transcription may be maintained on the centralized recordings index.

6.8 The department that creates the recording or transcription is the custodian of the recording. Custodians must retain recordings based upon retention schedules adopted pursuant to Administrative Procedure 6-3.

7. <u>RESPONSIBILITIES</u>

7.1 Department of Technology and Enterprise Business Solutions (TEBS)

7.1.1 Provide a 24-hour, 7 day-a-week secure, high-speed enterprise connection to Internet, intranet, and email services.

7.1.2 Notify Users of County Technology when particular services are or will be unavailable for system or network maintenance.

7.1.3 Accept help desk calls when a User notes a problem with County Technology, and distribute information, updates, and/or resolutions, as appropriate.

7.1.4 Provide the CIO (or designee) approval or denial of a department head's request to monitor a User's use of County Technology, or to access User Content.

7.1.5 Provide information to a department head regarding an employee's use of County Technology when directed by the CIO or designee to do so.

7.2 Department

7.2.1 Ensure that Users affiliated with the department are informed of, and comply with, this Administrative Procedure.

7.2.2 Ensure the appropriate use and connectivity of County Technology.

7.2.3 Ensure that this Administrative Procedure is incorporated by reference into all contracts in which the County is to provide contactors or volunteers with the use of County Technology to conduct the County's business, and that all contractors and volunteers are bound to comply with this Administrative Procedure.

7.2.4 A department head must seek and obtain approval from the CIO or designee prior to monitoring or accessing User Content.

7.2.5 Seek and obtain approval from TEBS before purchasing or connecting a device, application, or cloud service to the County Network.

7.3 County Employees

7.3.1 Keep apprised of the latest version of this Administrative Procedure.

7.3.2 Ensure use and connectivity of County Technology are in accordance with this Administrative Procedure.

7.3.3 Must not access another User's email or other account without written authorization from the department head.

7.3.4 In accordance with County information technology policies and procedures, obtain approval from the department head and the CAO or their designee before sending a broadcast electronic communication to all, or the majority of, County Technology Users.

8. PROCEDURE

8.1 General

8.1.1 **Employee** - Abide by this Administrative Procedure as it relates to the use and connectivity of County Technology.

8.1.2 **Department** - Ensure that all Users affiliated with the department are informed of and abide by this Administrative Procedure.

8.2 Broadcast email

8.2.1 **User** - Request approval from department head for sending an electronic broadcast communication to all, or the majority of Users.

8.2.2 **Department** - Request approval from the CAO or designee prior to permitting a User to send a broadcast electronic communication to all, or the majority of, Users.

8.2.3 **CAO** - Approve or disapprove requests to send County-wide broadcast electronic messages.

8.3 Monitoring and Accessing Use

8.3.1 **Department** - Determine if there is a legitimate business purpose to monitor a User's account or to access User Content.

If there is a legitimate business purpose to monitor a User/employee's use of County Technology, the department head must request in writing to the CIO or designee for approval to monitor User Content.

8.3.2 **CIO** - Approve or disapprove a department head's request for monitoring or accessing any User Content.

8.3.3 **TEBS** - For approved requests, provide appropriate information to the requesting department head.

9. DEPARTMENTS AFFECTED

9.1 All County departments.

OFFICE OF THE COUNTY EXECUTIVE

Marc Elrich
County Executive

Andrew W. Kleine
Chief Administrative Officer

MEMORANDUM

December 20, 2019

TO: Executive Branch Department and Office Directors,
MLS and Public Safety Managers
Administrative Services Coordinators and Functional Equivalents

FROM: Fariba Kassiri, Deputy Chief Administrative Officer

SUBJECT: Administrative Procedure 6-7, Information Security

The attached Administrative Procedure (AP) 6-7 establishes final policies and procedures for compliance with Information Security policy in the use of the County's computing assets and infrastructures. It is effective immediately to all County departments, offices, employees, volunteers, contractors and business partners.

The Chief Administrative Officer (CAO) has determined that the issuance of this revised AP 6-7 is necessary because the County's technology investment has grown significantly since the last policy update and the information security threat landscape has extended, and continues to extend, beyond the dimensions of computing investments and practices covered by the current policy. While the County continues to invest in technical security controls, experience shows that we, individually and collectively, as the users of technology are key to the success of the County's efforts to protect information in the County's possession including the information pertaining to the workforce, constituents, business partners, and volunteers, and to comply with the law, including laws recently passed or updated by the State and Federal governments.

AP 6-7 incorporates the recommendations of the CAO's Information Technology Policy Advisory Committee (IPAC) and uses a concise three-part format that is easy to reference, understand and implement by non-technical and technical audiences: AP 6-7 (3 pages); the Rules of Behavior Handbook (2 pages) and the System and Data Owners' Handbook (32 pages).

Interim AP 6-7 was issued on March 5, 2019. Based on comments and questions received following issuance of the interim AP, various provisions of the interim AP were clarified. The final AP 6-7 will be placed on the OMB Sharepoint site at: https://omb.mcgov.org/administrative-procedures/.

Attachments: Administrative Procedure 6-7, Information Security
Information Security Rules of Behavior Handbook
Information Security System and Data Owners Handbook

MONTGOMERY COUNTY ADMINISTRATIVE PROCEDURE

Offices of the County Executive • 101 Monroe Street • Rockville, Maryland 20850

NO.	6-7
PAGE	1 OF 5
DATE	12/20/2019
CAO APPROVAL	

Information Security

PURPOSE

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

DEFINITIONS

2.0 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, 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).

2.1 Department of Technology Services (DTS) – An Executive Branch department responsible for County Government enterprise information systems and telecommunications.

2.2 Enterprise Information Security Office EISO – An office within DTS that is responsible for the security of the County's Information System(s).

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

2.4 Information System Registry a central repository containing information on Information System(s).

2.5 Users – Individual or (system) process acting on behalf of an individual, authorized to access a system.

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

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 departments' Users procedures that implement this Administrative Procedure and associated Handbooks.

3.4 Compliance–Mandated Departments, 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 DTS 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:

3.5.1 Information Access Control

3.5.2 Information Security Awareness and Training

3.5.3 Audit and Accountability

3.5.4 Information Security Assessment, Authorization and Monitoring

3.5.5 Configuration Management

3.5.6 Contingency Planning

3.5.7 Identification and Authentication

3.5.8 Incident Response

3.5.9 Maintenance

3.5.10 Media Protection

3.5.11 Physical and Environmental Protection

3.5.12 Planning

3.5.13 Personnel Security

3.5.14 Risk Assessment

3.5.15 System and Services Acquisition

3.5.16 System and Communication Protection

3.5.17 System and Information Integrity

3.5.18 Program Management

3.5.19 Exemption from Administrative Procedure

3.6 Exemptions – Any deviations from this policy, including Information Security Rules of Behavior Handbook and Information Security System and Data Owners Handbook, require an Exemption Request to be submitted in writing by the Using Department and approved in by DTS EISO. 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. DTS EISO must track and report on exemptions granted.

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

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

3.9 Violation of this 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 Personnel laws and regulations, the Ethics Laws, currently codified at Chapter 33, COMCOR Chapter 33, and Chapter 19A of the County Code, 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 System(s), 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 Information Systems, or otherwise work on or interface with Information Systems, and must ensure that the 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 Procedure (AP 6–7), which is attached to, incorporated by reference into, and made a part of this contract.

RESPONSIBILITIES

4.1 User – User uses 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 train 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 contracts if a contractor's employees or its agents are provided access to the Information Systems.

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

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

4.2.7 Assists DTS with maintaining Information Systems in compliance with this administrative procedure.

4.2.8 Ensures that all Information Systems are registered with DTS and updated annually.

4.2.9 Reports on compliance to handbooks as referenced in the Information Security Rules of Behavior Handbook and the Information Security System and Data Owners Handbook.

4.3 DTS

4.3.1 Provides information security awareness training.

4.3.2 Reports Information Security risk and compliance status to the CAO.

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 Information Systems.

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

4.3.7 Leads investigations and responses to Information System security incidents.

4.3.8 Monitors Information System security threats and manages countermeasures.

4.3.9 Reviews Information System solicitations/contracts for inclusion of Information Security procedure and policy.

4.3.10 Performs/Evaluates Risk Assessments for all new Information Systems, and periodically for all existing Information Systems identified as critical/sensitive by the Using Department and or DTS.

4.3.11 Maintains and implements enterprise Information System security measures; 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 AP.

DEPARTMENTS AFFECTED

5.1 All Executive Branch departments and offices

APPENDICES

6.1 Information Security Rules of Behavior Handbook

6.2 Information Security System and Data Owners Handbook

1.0 Introduction and Purpose

The Information Security Rules of Behavior Handbook describes the rules associated with user's responsibilities and certain expectations of behavior using 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 Information Systems and applies to all County employees, volunteers, interns, contractors, and business partners at all times, regardless of how or where they are accessing the Information Systems.

2.0 Definitions

2.0 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, 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).

2.1 Department of Technology Services (DTS) – An Executive Branch department responsible for County Government enterprise information systems and telecommunications.

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

2.3 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 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.

2.4 Users – Individual, or (system) process acting on behalf of an individual, authorized to access a system.

3.0 Information Security Rules of Behavior

3.1 General

3.1.1 Any Information that is contained in, or stored on Information Systems, or transmitted, or received using Information Systems, is the property of the County and, therefore, is not private.

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

3.1.3 Users teleworking at any alternate workplace must follow security practices that are the same as or equivalent to those required at the primary workplace.

3.1.4 Users must only use County provided and approved infrastructure or cloud solutions for conducting County business and storing County information.

3.1.5 Users must use only the County-provided email / calendaring / collaboration solution (Office 365) for County work; forwarding of a County business email to a User's personal email system is prohibited.

3.2 When accessing or using Information Systems, Users must comply with the following:

3.2.1 Users must only access Information Systems and Information that is required in the performance of their official duties.

3.2.2 Users must promptly report any observed or suspected security problems/incidents, including loss/theft of Information Systems, or persons requesting that user to reveal their password.

3.2.3 Users must protect Sensitive Information per departmental procedures and report access, copying, or use of Sensitive Information that is not necessary to perform the User's County-assigned responsibilities.

3.2.4 Users must protect Information Systems from theft, destruction, or misuse.

3.2.5 Users must abide by software copyright laws.

3.2.6 Users must promptly change a password whenever it is compromised or suspected to be compromised.

3.2.7 Users must maintain the confidentiality of passwords and are responsible for actions performed with their accounts.

3.2.8 Users must lock Information Systems with a password when away from the work area (on–site and off–site), including for meals, breaks, or any extended period.

3.2.9 Users must physically protect Information Systems when used for teleworking and even when not in use.

3.2.10 Users must report unauthorized personnel that appear in the work area.

3.2.11 Users must protect Sensitive Information stored on electronic media, or in any physical format, such as paper, must lock the information in a secure area when not in use, and must delete, reformat, or shred Sensitive Information when it is no longer needed.

3.3 When accessing or using Information Systems, Users must not engage in the following activities:

3.3.1 Users must not write, display, or store passwords where others may access or view them.

3.3.2 Users must not 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.

3.3.3. Users must not obtain, install, replicate, or use unlicensed software unless authorized by their Department.

3.3.4 Users must not open emails from suspicious sources.

3.3.5 Users must not 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.

3.3.6 Users must not acquire, possess, or use hardware or software tools that defeat software copy protection, discover passwords, identify security vulnerabilities, or circumvent encryption.

3.3.7 Users must not attempt unauthorized access to an Information System, including attempt to access the information contained within the system.

3.3.8 Users must not use copyrighted or otherwise legally protected material without permission.

3.3.9 Users must not transmit chain letters, unauthorized mass mailings, or intentionally send malware.

3.3.10 Users must not use any personal computers/devices for County business or Information System that show signs of being infected by a virus or other malware.

3.3.11 Users must report any suspected information security incident to the IT Help Desk.

3.3.12 The County will determine and provide approved and authorized hardware or peripheral devices to documented, authorized Users. General Users may not add any devices to the County network without permission from County management.

3.3.13 Users must not alter hardware or software settings on any Information Systems without permission.

3.3.14 Users must not authorize or make a ransom payment.

Information Security System and Data Owners Handbook

December 12, 2019

Table of Contents

Chapter 1 – Information System Access Control AC 15
1.1 User Account Management AC-2 15
1.2 Access Enforcement AC-3 15
1.3 Least Privilege AC-6 15
1.4 Unsuccessful Logon Attempts AC-7 16
1.5 Information System Use Notification AC-8 16
1.6 Permitted Actions Without Identification or Authentication AC-14 16
1.7 Remote Access AC-17 16
1.8 Wireless Access AC-18 17
1.9 Access Control for Mobile Devices AC-19 17
1.10 Use of External Information Systems AC-20 17
1.11 Publicly Accessible Content AC-22 17
1.12 Sensitive Information Access (COUNTY ADDED) 17
1.13 Device Lock AC-11 17
Chapter 2 – Security Awareness and Training AT 18
2.1 Information Security Awareness Training AT-2 18
2.2 Role-Based Training AT-3 18
2.3 Information Security Training Records AT-4 18
Chapter 3 – Audit and Accountability AU 18
3.1 Audit Events AU-2 18
3.2 Content of Audit Records AU-3 18
3.3 Audit Storage Capacity AU-4 19
3.4 Response to Audit Processing Failures AU-5 19
3.5 Audit Review, Analysis, and Reporting AU-6 19
3.6 Time Stamps AU-8 19
3.7 Protection of Audit Information AU-9 19
3.8 Audit Record Retention AU-11 19
3.9 Audit Generation AU-12 19
Chapter 4 – Information Security Assessments and Privacy Assessments, Authorization, and Monitoring CA 20
4.1 Security Controls Assessments and Privacy Controls Assessments CA-2 20
4.2 Information System Interconnections CA-3 20
4.3 Plan of Action and Milestones (POAMS) CA-5 20
4.4 Information System Authorization CA-6 21
4.5 Continuous Monitoring/Risk Monitoring CA-7 21

4.6 Penetration Testing CA-8 21

4.7 Internal Information System Connections CA-9 21

4.8 Information System Registration (COUNTY ADDED) 21

Chapter 5 – Configuration Management CM 21

5.1 Baseline Configuration CM-2 22

5.2 Configuration Change Control CM-3 22

5.3 Security Impact Analyses and Privacy Impact Analyses CM-4 22

5.4 Access Restrictions for Change CM-5 22

5.5 Configuration Settings CM-6 22

5.6 Least Functionality CM-7 23

5.7 Information System Component Inventory CM-8 23

5.8 Software Usage Restrictions CM-10 23

5.9 User-Installed Software CM-11 23

Chapter 6 – Contingency Planning CP 24

6.1 Contingency Plan CP-2 24

6.2 Contingency Training CP-3 24

6.3 Contingency Plan Testing CP-4 25

6.4 Alternate Storage Site CP-6 25

6.5 Alternate Processing Site CP-7 25

6.6 Information System Backup CP-9 25

6.7 Information System Recovery and Reconstitution CP-10 26

Chapter 7 – Identification and Authentication IA 26

7.1 Identification and Authentication (County Users) IA-2 26

7.2 Identification and Authentication (County Users) | Multifactor Authentication to Information System User Accounts IA-2(1) 26

7.3 Identification and Authentication (County Users) | Access to Accounts – Replay Resistant IA-2(8) .. 26

7.4 Identifier Management IA-4 26

7.5 Authenticator Management IA-5 26

7.6 Authenticator Feedback IA-6 27

7.7 Cryptographic Module Authentication IA-7 27

7.8 Identification and Authentication (Non-County Users – Business Partners) IA-8 27

7.9 Re-Authentication IA-11 27

Chapter 8 – Incident Response 28

8.1 Incident Response (IR) Training IR-2 28

8.2 Incident Handling IR-4 28

8.3 Incident Monitoring IR-5 28

8.4 Incident Reporting IR-6 28

8.5 Incident Response Assistance IR-7 28
8.6 Incident Response Plan IR-8 29
Chapter 9 – Maintenance MA 29
9.1 Controlled Maintenance MA-2 29
9.2 Nonlocal Maintenance MA-4 30
9.3 Maintenance Personnel MA-5 30
Chapter 10 – Media Protection MP 30
10.1 Media Access MP-2 30
10.2 Media Storage MP-4 30
10.3 Media Transport MP-5 31
10.4 Media Sanitization MP-6 31
10.5 Media Use MP-7 31
Chapter 11 – Physical and Environmental Protection PE 31
11.1 Physical Access Authorizations PE-2 31
11.2 Physical Access Control PE-3 31
11.3 Monitoring Physical Access PE-6 32
11.4 Visitor Access Records PE-8 32
11.5 Emergency Lighting PE-12 32
11.6 Fire Protection PE-13 32
11.7 Temperature and Humidity Controls PE-14 32
11.8 Water Damage Protection PE-15 33
11.9 Delivery and Removal PE-16 33
11.10 Alternate Work Site PE-17 33
11.11 Emergency Power Control/ Electromagnetic Pulse Protection PE-11/PE-21 33
Chapter 12 – Planning PL 33
12.1 Information Security and Privacy Plans PL-2 33
12.2 Rules of Behavior PL-4 34
Chapter 13 – Personnel Security PS 34
13.1 Position Risk Designation PS-2 34
13.2 Personnel Screening PS-3 34
13.3 Personnel Termination PS-4 34
13.4 Personnel Transfer PS-5 35
13.5 Personnel Security PS-1 & PS-7 35
13.6 Personnel Sanctions PS-8 35
Chapter 14 Risk Assessment RA 35
14.1 Security Categorization RA-2 35
14.2 Risk Assessment RA-3 36

14.3 Vulnerability Scanning of Information Systems RA-5 36
14.4 Risk Response RA-7 37
14.5 Risk Assignment (COUNTY ADDED) 37
Chapter 15 – Information System and Services Acquisition SA 37
15.1 Allocation of Resources SA-2 37
15.2 Information System Development Life Cycle SA-3 38
15.3 Acquisition Process SA-4 38
15.4 Information System Documentation SA-5 38
15.5 Security and Privacy Engineering Principles SA-8 39
15.6 Unsupported Information System Components SA-22 39
Chapter 16 – Information System and Communications Protection SC 39
16.1 Denial of Service Protection SC-5 39
16.2 Boundary Protection SC-7 39
16.3 Cryptographic Key Establishment and Management SC-12 39
16.4 Cryptographic Protection SC-13 39
16.5 Collaborative Computing Devices and Applications SC-15 39
16.6 Secure Name/Address Resolution Service SC-20 & SC-21 40
16.7 Process Isolation SC-39 40
Chapter 17 – Information System and Information Integrity 40
17.1 Flaw Remediation SI-2 40
17.2 Malicious Code Protection SI-3 40
17.3 Information System Monitoring SI-4 40
17.4 Security Alerts, Advisories, and Directives SI-5 41
17.5 Information Management and Retention SI-12 41
Chapter 18 – Program Management PM 41
18.1 Information System Inventory PM-5 41
18.2 Enterprise Architecture PM-7 41
18.3 Registration Process PM-10 (COUNTY ADDED) 41
18.4 Security and Privacy Workforce PM-13 42
18.5 Contacts with Groups and Associations PM-15 42
18.6 Minimization of Personally Identifiable Information Used in Testing, Training, and Research PM-26 42
18.7 Inventory of Personally Identifiable Information PM-29 42
Chapter 19 – Exemption from Administrative Procedure 42

Record of Changes

Date	Description	Version	Author

Revision History

Date	Description	Version	Author
11/22/18	Drafted by DTS and recommended to CAO as Interim procedure	0.1	Angel Stanley
3/25/19	Resolved all attorney's questions	0.2	Joyce Graham
5/1/19	Final with CAO and CISO updates	0.3	Joyce Graham
6/10/19	Department edits added	0.4	Joyce Graham
8/1/19	Final	1.0	Keith Young

Introduction and 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 and adaptable to state, local and private sector organization's Information Resources.

This hand book has been developed as a support document to AP 6-7, Policy 3.5 that states:

> DTS 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.
>
> 3.5.1 Information Access Control
> 3.5.2 Information Security Awareness and Training
> 3.5.3 Audit and Accountability
> 3.5.4 Information Security Assessment, Authorization, and Monitoring
> 3.5.5 Configuration Management
> 3.5.6 Contingency Planning
> 3.5.7 Identification and Authentication
> 3.5.8 Incident Response
> 3.5.9 Maintenance
> 3.5.10 Media Protection
> 3.5.11 Physical and Environmental Protection
> 3.5.12 Planning
> 3.5.13 Personnel Security
> 3.5.14 Information System Risk Assessment
> 3.5.15 Information System and Services Acquisition
> 3.5.16 Information System and Communication Protection
> 3.5.17 Information System and Information Integrity
> 3.5.18 Program Management
> 3.5.19 Exemption from Administrative Procedure

Scope

The Montgomery County Information Security System and Data Owners Handbook (ISSaDO 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.

Definitions

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.

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.

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.

Department of Technology Services (DTS) – An Executive Branch Department that is responsible for County Government enterprise Information Systems and telecommunications.

Effectiveness Monitoring – A process that determines the ongoing efficiency of implemented Risk Response measures.

Enterprise Information Security Office (EISO) – An office within DTS that is responsible for the security of the County's Information System(s).

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.

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.

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.

Multifactor (Two Factor) Authentication – An authentication system or an authenticator that requires more than one authentication factor for successful authentication. Multifactor authentication can be performed using a single authenticator that provides more than one factor or by a combination of authenticators that provide different factors. The three authentication factors are something you know, something you have, and something you are.

Nonlocal Maintenance – Nonlocal Maintenance and diagnostic activities are those activities conducted by individuals communicating through a network, either an external or internal network.

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.

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 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 number;
   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.

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

User or Information System User – Individual or (system) process acting on behalf of an individual, authorized to access a system.

> **County User** – A County employee or an individual the County deems to have equivalent status of an employee including, for example, contractor, guest researcher, individual detailed from another entity. Policy and procedures for granting equivalent status of employees to individuals may include need-to-know, relationship to the County, and citizenship.
>
> **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 path.

Chapter 1 – Information System Access Control AC

1.1 User Account Management AC-2

Information System Owners must:

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;

1.1.2 Assign account managers for all User or Service Accounts;

1.1.3 Establish conditions for group and role membership;

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;

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

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

1.1.7 Monitor the use of User accounts;

1.1.8 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;

1.1.9 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 DTS or associated missions and business functions;

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

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

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

1.2 Access Enforcement AC-3

1.2.1 Information System Owners must enforce approved authorization for Logical Access to Information Systems.

1.3 Least Privilege AC-6

Information System Owners must ensure that access to Information Systems is secure, by taking measures that include the following:

1.3.1 Employ the principle of Least Privilege within the environment allowing only Authorized Accesses for Users (or automated Information System processes acting on behalf of Users) which are necessary to accomplish assigned tasks in accordance with County missions and business functions.

1.3.2 Reviews of the privileged accounts must be performed annually to validate the need for such privileges.

1.3.3 Privileges must be removed or reassigned, if necessary, to correctly reflect the County mission and business needs.

1.3.4 Assign staff to perform an audit of privileged Information System account functions.

1.4 Unsuccessful Logon Attempts AC-7

Information System Owners must:

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

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.

1.5 Information System Use Notification AC-8

1.5.1 County Information Systems must 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:

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

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.

1.6 Permitted Actions Without Identification or Authentication AC-14

Information System Owners must:

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).

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

1.7 Remote Access AC-17

1.7.1 DTS must establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of Remote Access allowed to an Information System.

To have Remote Access to Information Systems, a User and/or a Department must do the following:

1.7.2 County-Sensitive Information may not be stored on non-County controlled resources unless all Department and DTS procedures in this handbook, all federal, state, and County laws and policies are followed.

1.8 Wireless Access AC-18

1.8.1 DTS 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.

1.9 Access Control for Mobile Devices AC-19

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

1.9.2 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.

1.9.3 The County is not responsible for maintenance, damage, or loss of personally-owned computers, data, or peripherals used by employees in the work place.

1.9.4 A User 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.

1.10 Use of External Information Systems AC-20

1.10.1 DTS must establish terms and conditions for authorized individuals accessing County Information Systems from External or Third-Party Information Systems.

1.11 Publicly Accessible Content AC-22

1.11.1 The County and its individual Information System Owners 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.

1.12 Sensitive Information Access (COUNTY ADDED)

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

1.13 Device Lock (AC-11 COUNTY ADDED – Not in NIST LOW)

1.13.1 To protect Sensitive Information, a User must not leave the PC terminal area while Sensitive Information 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, installed on the PC that blanks the screen until the correct password, is entered.

Chapter 2 – Security Awareness and Training AT

2.1 Information Security Awareness Training AT-2

The County must:

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

2.1.2 Train when required by Information System changes; and

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

2.2 Role-Based Training AT-3

Information System Owners must 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):

2.2.1 Before authorizing access to the Information System or performing assigned duties;

2.2.2 When required by Information System changes; and

2.2.3 On a regularly scheduled basis.

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

The County must document and monitor basic Information Security awareness training activities.

Information System Owners must:

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

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

Chapter 3 – Audit and Accountability AU

3.1 Audit Events AU-2

Information System Owners must:

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.)

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

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

3.1.4 Audit and document the subset auditable events determined from Audit Event - (3.1.1) monthly.

3.2 Content of Audit Records AU-3

3.2.1 Information System Owners must 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

3.3 Audit Storage Capacity AU-4

3.3.1 Information System Owners must allocate Audit Record storage capacity to accommodate the Audit Record retention requirements.

3.4 Response to Audit Processing Failures AU-5

Information System Owners must:

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

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

3.5 Audit Review, Analysis, and Reporting AU-6

Information System Owners must:

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

3.5.2 Report findings to designated personnel; and

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.

3.6 Time Stamps AU-8

Information System Owners must:

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

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.

3.7 Protection of Audit Information AU-9

3.7.1 Information System Owners must protect audit information and audit tools from unauthorized access, modification, and deletion.

3.8 Audit Record Retention AU-11

3.8.1 Information System Owners must 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.

3.9 Audit Generation AU-12

Information System Owners must:

3.9.1 Provide Audit Record generation capability for the auditable event types in Audit Event - (3.1.1) at all Information System Components where audit capability is deployed/available;

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

3.9.3 Generate Audit Records for the event types defined in Audit Event - (3.1.1) with the information in Content of Audit Record.

Chapter 4 – Information Security Assessments and Privacy Assessments, Authorization, and Monitoring CA

4.1 Security Controls Assessments and Privacy Controls Assessments CA-2

DTS must:

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 controls effectiveness;
3. Assessment environment and Assessment team;

4.1.2 Ensure the Security Controls Assessment Plan and Privacy Controls Assessment Plan are reviewed and approved by the designated EISO County representative prior to retaining an independent Assessor to conduct the Assessments;

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;

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.

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

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.

4.2 Information System Interconnections CA-3

The County must:

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

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

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

4.3 Plan of Action and Milestones (POAMS) CA-5

DTS must:

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 4.1.4 and 4.1.5, or otherwise identified, to reduce or eliminate known vulnerabilities in Information Systems;

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.

4.4 Information System Authorization CA-6

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

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 DTS is prohibited.

4.5 Continuous Monitoring/Risk Monitoring CA-7

4.5.1 DTS must 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

4.6 Penetration Testing CA-8 (COUNTY ADDED – Not in NIST LOW)

4.6.1 DTS must perform Penetration Testing every three (3) years on Information Systems with High Risks.

4.7 Internal Information System Connections CA-9

The County must:

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

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

4.8 Information System Registration (COUNTY ADDED)

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 DTS 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.

Chapter 5 – Configuration Management CM

5.1 Baseline Configuration CM-2

Information System Owners must:

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

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.

5.2 Configuration Change Control CM-3

DTS must:

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

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

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:

5.2.4 Submit proposed configuration-controlled changes to the Information System to DTS for approval.

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

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

5.2.7 Report all configuration-controlled changes to the Information System to DTS prior to implementation

5.3 Security Impact Analyses and Privacy Impact Analyses CM-4

DTS must:

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

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.

The Information System Owners must:

5.3.2 Analyze the risk determination provided from DTS to decide whether to continue with the implementation or select an alternative implementation.

5.4 Access Restrictions for Change CM-5

5.4.1 Information System Owners must define, document, approve, and enforce physical and Logical Access restrictions associated with configuration-controlled changes to the Information Systems.

5.5 Configuration Settings CM-6

Information System Owners must:

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;

5.5.2 Implement the Configuration Settings;

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

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

5.6 Least Functionality CM-7

Information System Owners must:

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

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.

5.7 Information System Component Inventory CM-8

Information System Owners must:

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 DTS to achieve effective Information System Component accountability; and

5.7.2 Review and update the Information System Component inventory at least every six months.

5.8 Software Usage Restrictions CM-10

5.8.1 DTS, Departments, and Users must use any licensed software and associated documentation in accordance with all applicable contractual terms, including, without limitation, any software license agreements.

5.8.2 To the extent a contract or software license agreement tracks use by quantity of Users or other numeric value, DTS and Departments must 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.

5.8.3 Information System Owners must 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.

5.9 User-Installed Software CM-11

DTS must:

5.9.1 Establish policies governing the installation of software by Users;

5.9.2 Enforce software installation policies; and

5.9.3 Monitor policy compliance continuously.

Chapter 6 – Contingency Planning CP

6.1 Contingency Plan CP-2

Information System Owners must:

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 DTS.

6.1.2 Distribute copies of the Contingency Plan to key contingency personnel.

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

6.1.4 Review the Contingency Plan for the Information System at least annually

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;

6.1.6 Communicate Contingency Plan changes to key contingency personnel; and

6.1.7 Protect the Contingency Plan from unauthorized disclosure and modification.

6.2 Contingency Training CP-3

Information System Owners must:

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

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.

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

6.3 Contingency Plan Testing CP-4

Information System Owners must:

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;

6.3.2 Review the Contingency Plan Test Results; and

6.3.3 Initiate corrective actions, if needed.

6.4 Alternate Storage Site CP-6

DTS, Departmènt of Police Security Services, and the Department of General Services must:

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,

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

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:

6.4.4 Backup crucial data and files 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.

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

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.

6.4.7 Notify DTS as soon as changes in facilities are determined.

6.5 Alternate Processing Site CP-7 (COUNTY ADDED – Not in NIST LOW)

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

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

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

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

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

6.6 Information System Backup CP-9

Information System Owners must:

6.6.1 Conduct daily Incremental Backups and weekly Full Backups of User-Level Information contained in the Information System;

6.6.2 Conduct daily Incremental Backups and weekly Full Backups of Information System-Level Information contained in the Information System;

6.6.3 Conduct daily Incremental Backups and weekly Full Backups of Information System documentation including security-related documentation and;

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

6.7 Information System Recovery and Reconstitution CP-10

Information System Owners must:

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

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

Chapter 7 – Identification and Authentication IA

7.1 Identification and Authentication (County Users) IA-2

7.1.1 Information System Owners must uniquely identify and authenticate Users or automated Information System processes (Service Accounts) acting on behalf of County Users.

7.2 Identification and Authentication (County Users) | Multifactor Authentication to Information System User Accounts IA-2(1)

7.2.1 Information System Owners must implement multifactor authentication for access to User Accounts, including both privileged and non-privileged Accounts.

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

7.3.1 Information System Owners must implement replay-resistant authentication mechanisms for access to privileged Accounts.

7.4 Identifier Management IA-4

Information System Owners must manage Information System Identifiers by:

7.4.1 Receiving authorization from designated personnel to assign an individual, group, role, or device Identifier;

7.4.2 Selecting an Identifier that identifies an individual, group, role, or device;

7.4.3 Assigning the Identifier to the intended individual, group, role, or device; and

7.4.4 Preventing reuse of Identifiers for 180 days.

7.5 Authenticator Management IA-5

Information System Owners must manage Information System Authenticators by:

7.5.1 Verifying, as part of the initial Authenticator distribution, the identity of the individual, group, role, or device receiving the Authenticator;

7.5.2 Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;

7.5.3 Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;

7.5.4 Changing/refreshing authenticators every ninety (90) days.

7.5.5 Authenticators must be at least eight (8) characters in length, 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.

7.5.6 Protecting authenticator content from unauthorized disclosure and modification;

7.5.7 Requiring individuals to take, and having devices implement, specific security controls to protect authenticators; and

7.5.8 Changing authenticators for group/role accounts when membership to those accounts changes.

For password-based authentication, Information System Owners must: **IA-5(1)**

7.5.9 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;

7.5.10 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;

7.5.11 Transmit only cryptographically-protected passwords;

7.5.12 Store passwords using a DTS approved-hash algorithm

7.5.13 Require immediate selection of a new password upon Account recovery;

7.5.14 Allow User selection of long passwords and passphrases, including spaces and all printable characters; and

7.5.15 Employ automated tools to assist the User in selecting strong password Authenticators.

7.6 Authenticator Feedback IA-6

7.6.1 Information System Owners must obscure feedback of authentication information during the authentication process to protect the information from possible exploitation and use by unauthorized individuals.

7.7 Cryptographic Module Authentication IA-7

Information System Owners must:

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.

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

7.8.1 Information System Owners must uniquely identify and authenticate non-County Users or automated Information Systems acting on behalf of non-County Users.

7.9 Re-Authentication IA-11

7.9.1 Information System Owners must require Users to re-authenticate when passwords have expired, and new passwords are created.

Chapter 8 – Incident Response

8.1 Incident Response (IR) Training IR-2

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

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.

8.2 Incident Handling IR-4

EISO must:

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

8.2.2 Coordinate incident handling activities with Contingency Planning activities;

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

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:

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

8.3 Incident Monitoring IR-5

8.3.1 EISO must track and document Information System security and privacy incidents.

8.4 Incident Reporting IR-6

Information System Owners must:

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

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

EISO must:

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

8.5 Incident Response Assistance IR-7

8.5.1 EISO and other key players per EISO Incident Response Plan must 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.

8.6 Incident Response Plan IR-8

EISO must:

8.6.1 Develop an Incident Response Plan that:

1. Identifies the following:
    a. Preparing for an incident;
    b. Identifying and 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 affect 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.

8.6.2 Distribute copies of the incident response plan to designated incident response personnel within DTS and Departments;

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

8.6.4 Communicate Incident Response Plan changes to DTS and Departments; and

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

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.

Chapter 9 – Maintenance MA

9.1 Controlled Maintenance MA-2

For non-cloud-based Information Systems, Information System Owners must:

9.1.1 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;

9.1.2 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;

9.1.3 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;

9.1.4 Sanitize equipment to remove all information from associated media prior to removal from County facilities for off-site maintenance, repair, or replacement;

9.1.5 Check all potentially impacted security and privacy controls to verify that the controls are still functioning properly following maintenance, repair, or replacement actions; and

9.1.6 Include in County maintenance records response times for service, if possible, when repairing a network server.

9.2 Nonlocal Maintenance MA-4

For non-cloud-based Information Systems, Information System Owners must:

9.2.1 Approve and monitor Nonlocal Maintenance and diagnostic activities performed by the County's vendors.

9.2.2 Allow the use of Nonlocal Maintenance and diagnostic tools only as consistent with County policy.

9.2.3 Employ strong Authenticators in the establishment of Nonlocal Maintenance and diagnostic sessions;

9.2.4 Maintain records for Nonlocal Maintenance and diagnostic activities; and

9.2.5 Terminate session and network connections when Nonlocal Maintenance is completed.

9.3 Maintenance Personnel MA-5

Information System Owners must:

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

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

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.

Chapter 10 – Media Protection MP

10.1 Media Access MP-2

10.1.1 DTS must 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).

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

10.1.3 Information System Owners must define types of restricted digital and/or non-digital media and restrict the access.

10.2 Media Storage MP-4

10.2.1 Information System Owners must 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.

10.3 Media Transport MP-5

Information System Owners must:

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;

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

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

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

10.4 Media Sanitization MP-6

Information System Owners must:

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

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

10.5 Media Use MP-7

DTS must:

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, detection software devices;

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

Chapter 11 – Physical and Environmental Protection PE

11.1 Physical Access Authorizations PE-2

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

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:

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

11.1.3 Authorization credentials must be issued for facility access.

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

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

11.2 Physical Access Control PE-3

Department of General Services and Department of Police Security Services must

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

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.

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

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

11.2.5 Inventory County defined physical access devices annually;

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

11.3 Monitoring Physical Access PE-6

11.3.1 Department of General Services and Department of Police Security Services must periodically inspect environment and safety of Information Systems by qualified personnel to ensure the safety of Information Systems.

11.3.2 Information System Owners must monitor and review physical access to the facility where the Information Systems resides to detect and respond to physical security incidents.

11.4 Visitor Access Records PE-8

11.4.1 Information System Owners must maintain and review visitor access records to the non-public sections of the facility where the Information Systems resides.

11.5 Emergency Lighting PE-12

11.5.1 DTS and the Department of General Services must 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.

11.6 Fire Protection PE-13

Department of General Services must:

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

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:

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

11.7 Temperature and Humidity Controls PE-14

11.7.1 Department of General Services must maintain and monitor temperature and humidity levels within the facility where the Information Systems resides to ensure the safety of the Information Systems.

11.8 Water Damage Protection PE-15

11.8.1 Department of General Services must protect the Information Systems from damage resulting from water leakage by providing master shutoff or isolation valves.

11.8.2 Information System Owners must ensure that alternate work site facilities protect against water damage to ensure the safety of Information Systems.

11.9 Delivery and Removal PE-16

11.9.1 Information System Owners must authorize, monitor, and control Information System Components entering and exiting the facility and maintain records of those items.

11.10 Alternate Work Site PE-17

Departments must:

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

11.10.2 Employ the same EISO security and privacy controls at alternate work site.

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

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

11.11 Emergency Power Control/ Electromagnetic Pulse Protection PE-11/PE-21

11.11.1 Department of General Services must 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.

Chapter 12 – Planning PL

12.1 Information Security and Privacy Plans PL-2

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

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 rational for the tailoring decisions; and
9. Are reviewed and approved by a designated official or designated representative prior to plan implementation;

12.1.2 Distribute copies of the security and privacy plans and communicate subsequent changes to the plans to DTS;

12.1.3 Review the security and privacy plans at least annually;

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

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

12.2 Rules of Behavior PL-4

EISO and Information System Owners must:

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;

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

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

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 Internet, Intranet, and Electronic Mail Services." As noted in Administrative Procedure 6-1, all use must comply with all applicable laws and policies.

Chapter 13 – Personnel Security PS

13.1 Position Risk Designation PS-2

Departments must:

13.1.1 Assign a risk designation to all County positions

13.1.2 Establish screening criteria for individuals filling those positions; and

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

13.2 Personnel Screening PS-3

Departments must:

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

13.2.2 Rescreen individuals in accordance with specific departmental requirements.

13.3 Personnel Termination PS-4

Departments must, upon termination of User employment:

13.3.1 Disable Information System access within the same day;

13.3.2 Terminate or revoke any Authenticators and credentials associated with the User;

13.3.3 If possible, conduct exit interviews that include a discussion of departmentally defined Information Security topics;

13.3.4 Retrieve all security-related County Information System-related property;

13.3.5 Retain access to County information and Information Systems formerly controlled by terminated User; and

13.3.6 Notify the Help Desk per DTS policy within same day.

13.4 Personnel Transfer PS-5

Departments must:

13.4.1 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;

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

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

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

13.5 Personnel Security PS-1 & PS-7

Departments must:

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

13.5.2 Require all departmental and contracted personnel comply with personnel security policies and procedures established by the Departments;

13.6 Personnel Sanctions PS-8

Departments must:

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

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

Chapter 14 Risk Assessment RA

14.1 Security Categorization RA-2

Departments must:

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

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

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

14.2 Risk Assessment RA-3

EISO must:

14.2.1 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 EISO, 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;

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

14.2.3 Document Risk Assessment results in Risk Assessment reports;

14.2.4 Review Risk Assessment results annually;

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

14.2.6 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

14.3 Vulnerability Scanning of Information Systems RA-5

EISO must:

14.3.1 Scan for vulnerabilities at least monthly in the operating Information Systems/infrastructure, web applications and databases, and when new vulnerabilities potentially affecting the Information System are identified and reported;

14.3.2 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;

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

Information System Owners must:

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

14.3.5 Remediate High Risk Vulnerabilities immediately upon notification from EISO. Remediate Moderate Risk Vulnerabilities within thirty (30) days from date of discovery and Low Risk Vulnerabilities within ninety (90) days from date of discovery.

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

14.4 Risk Response RA-7

14.4.1 Departments must respond to findings from Security Controls Assessments and Privacy Controls Assessments, Risk Assessments, monitoring, and audits with Risk Mitigation plans. If the risk cannot be mitigated, the Department must notify DTS so that Risk Acceptance, Risk Avoidance, Risk Rejection, or Risk Transfer can be identified.

14.5 Risk Assignment (COUNTY ADDED – Not in NIST 800-53)

Risk will be assigned at the following levels

14.5.1 Information System Department Head

If the Department:

1. Fails to register an Information System with DTS, or
2. Fails to follow DTS recommendations for implementation/remediation, or
3. Fails to champion a budget request as a result of Security Controls Assessments or Privacy Controls Assessment.

14.5.2 Chief Information Officer in the Department of Technology Services (DTS)

If DTS:

1. Fails to perform a Risk Assessment, or
2. Fails to document, and/or not appropriately communicate Risk Assessment risks, or
3. Fails to submit a budget request following a risk identified from a Security and Privacy Assessment, or
4. If CIO accepts the risk(s) based on the Risk Assessment, priorities, constraints, and/or business need

14.5.3 Office of Management & Budget Director

If OMB, in its sole discretion:

1. Denies or partially funds requests to mitigate/resolve risks identified as the result of a Risk Assessment.

14.5.4 Chief Administrative Officer (CAO)

If the CAO:

1. Accepts the risk(s) based on the Risk Assessment, priorities, constraints, and business need

Chapter 15 – Information System and Services Acquisition SA

15.1 Allocation of Resources SA-2

The County must:

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

15.1.2 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

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

15.2 Information System Development Life Cycle SA-3

Information System Owners must:

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

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

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

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

15.3 Acquisition Process SA-4

15.3.1 The County must 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.

15.4 Information System Documentation SA-5

Information System Owners must:

15.4.1 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;

15.4.2. 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;

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

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

15.4.5 Distribute documentation to Department Heads and DTS EISO.

15.5 Security and Privacy Engineering Principles SA-8

15.5.1 Information System Owners must apply EISO security and privacy engineering principles, as defined in DTS architecture documents, in the specification, design, development, implementation, and modification of the Information System and components.

15.6 Unsupported Information System Components SA-22

15.6.1 Information System Owners must replace Information System Components when support for the components is no longer available from the developer, vendor, or manufacturer.

Chapter 16 – Information System and Communications Protection SC

16.1 Denial of Service Protection SC-5

16.1.1 DTS must protect against or limit the effects of Denial of Service events by employing security safeguards.

16.2 Boundary Protection SC-7

DTS must:

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

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

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.

16.3 Cryptographic Key Establishment and Management SC-12

16.3.1 Information System Owners must establish and manage Cryptographic Keys for required cryptography employed within Information System in accordance with EISO requirements for key generation, distribution, storage, access, and destruction.

16.4 Cryptographic Protection SC-13

16.4.1 DTS must implement defined cryptographic uses and type of cryptography for each use to ensure cryptographic protection of data.

16.5 Collaborative Computing Devices and Applications SC-15

DTS must:

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

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

16.6 Secure Name/Address Resolution Service SC-20 & SC-21

DTS must:

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

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

16.7 Process Isolation SC-39

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

Chapter 17 – Information System and Information Integrity

17.1 Flaw Remediation SI-2

Information System Owners must:

17.1.1 Identify, report, and correct Information System Flaws;

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

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

17.1.4 Incorporate Flaw remediation into DTS configuration management process.

17.2 Malicious Code Protection SI-3

DTS and Information System Owners must:

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;

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

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 alert to administrator; promptly in response to Malicious Code detection; and

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.

17.3 Information System Monitoring SI-4

EISO, and Information System Owners must:

17.3.1 Monitor the Information System to detect:

1. Attacks and indicators of potential attacks; and

2. Unauthorized local, network, and remote connections;

17.3.2 Identify unauthorized use of the Information System;

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;

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

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;

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

17.3.7 Provide Information System monitoring information to EISO.

17.4 Security Alerts, Advisories, and Directives SI-5

EISO must:

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

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

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:

17.4.4 Implement security directives in accordance with established time-frames, or

17.4.5 Notify EISO of the degree of noncompliance.

17.5 Information Management and Retention SI-12

17.5.1 Information System Owners must 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.

Chapter 18 – Program Management PM

18.1 Information System Inventory PM-5

18.1.1 Information System Owners must develop and maintain an inventory of Information Systems.

18.2 Enterprise Architecture PM-7

18.2.1 DTS must develop an enterprise architecture with consideration for information security, privacy, and the resulting Risk to County operations and assets, individuals, other organizations, and the Nation.

18.3 Registration Process PM-10 (COUNTY ADDED)

18.3.1 DTS must manage the security and privacy state of Information Systems and the environments in which those Information Systems operate through Information System registration.

18.4 Security and Privacy Workforce PM-13

18.4.1 The County must establish a security and privacy workforce development and improvement program.

18.5 Contacts with Groups and Associations PM-15

18.5.1 The County must 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.

18.6 Minimization of Personally Identifiable Information Used in Testing, Training, and Research PM-26

The County must:

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

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

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

18.7 Inventory of Personally Identifiable Information PM-29

DTS must:

18.7.1 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.

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

Information System Owners must:

18.7.3 Provide updates of the Personally Identifiable Information inventory to DTS as needed

18.7.4 Review the Personally Identifiable Information inventory as needed

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

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

Chapter 19 – Exemption from Administrative Procedure

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

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) that completed comparable training elsewhere within the past year. Exemption requests must be submitted to the EISO, and the Department Head must assume the risk.