

LICENSE AGREEMENT
BETWEEN
MONTGOMERY COUNTY, MARYLAND
AND
THE BALTIMORE THERAPY CENTER, LLC

DATE: October 5, 2021

TABLE OF CONTENTS

Paragraph

1. Licensed Premises
2. License Term
3. Early Termination
4. License Fee
5. Use Licensed Premises
6. Assignment
7. Condition of Licensed Premises
8. Alterations and Improvements
9. Liens
10. Services and Operating Expenses
11. Furniture, Fixtures and Equipment
12. Liability, Property Damage and Fire Insurance
13. Hold Harmless
14. Responsibilities of Licensee
15. Destruction of Licensed Premises
16. Default
17. Access
18. Surrender of Possession
19. Notice of Accidents, Defects or Damage
20. Compliance with Laws
21. Waiver
22. Non-Discrimination
23. Public Employment
24. Mailing Notices
25. Resident Agent
26. Prohibition of Hazardous Substances
27. Non-Appropriation
28. American Disabilities Act Requirements
29. Eminent Domain
30. Force Majeure
31. Entire Agreement
32. Modification
33. Governing Law
34. Claims
35. Holdover
36. No Tenancy Created

Exhibit A – Contract #1110701

Exhibit B – Licensed Premises

LICENSE AGREEMENT

THIS LICENSE AGREEMENT (the "License"), made this 5 day of October, 2021, by and between MONTGOMERY COUNTY, MARYLAND, a body corporate and politic (the "County") and THE BALTIMORE THERAPY CENTER, LLC. ("Licensee"), (the County and the Licensee together the "Parties").

WITNESSETH:

WHEREAS, the County is the owner of fee simple title in the improvements and contiguous grounds located at 8818 Georgia Avenue, Silver Spring, MD 20901 (the "Building"), and

WHEREAS, the County, through its Department of Health and Human Services, created a program of individual and group counseling services for domestic violence offenders through its Abuser Intervention Program. This program follows the Maryland State Operational guidelines for Abuser Intervention Programs.

WHEREAS, the County entered Contract Number #1110701 (the "Contract") with Licensee to support the above referenced programs, a copy of the Contract is attached hereto as Exhibit "A" and incorporated herein by reference.

WHEREAS, the County has agreed to license space in the Building for Licensee to provide the services defined in the Contract subject to the terms and conditions contained herein.

NOW THEREFORE, and in consideration of the covenants contained in this License, and for other good and valuable consideration, the receipt and sufficiency of which is acknowledged by the Parties, the Parties mutually agree as follows:

1. LICENSED PREMISES: The County does hereby grant the Licensee the privilege, license and right to use the offices on the second floor marked with an "X" and those shared conference rooms on the first floor in the Building (collectively the

“Licensed Premises”) all as shown on Exhibit “B” attached hereto and incorporated herein by reference.

2. LICENSE TERM: The License Term shall commence on December 1, 2020 and end on November 30, 2021 (License Term”). The License shall run concurrently with the Contract, as amended, and will terminate automatically upon the termination of the License Term and/or the Contract, unless this License is earlier terminated.

3. EARLY TERMINATION: It is agreed between the Parties that this License may be terminated at any time during the License Term or any extension of the License Term by either party giving thirty (30) days written notice of the termination. The County is under no obligation to provide alternate space for Licensee and is not responsible for any moving costs or any expenses incurred by Licensee to relocate or move whether such move or relocation is the result of termination or any other reason.

4. LICENSE FEE: In consideration of services provided by the Licensee as set forth in the Contract, and for the rights and obligations provided for in this License, Licensee shall pay to the County One Dollar (\$1.00) on the date this License is executed by the Parties, payable by check to: Montgomery County, Maryland, Department of General Services, Office of Real Estate, P.O. Box 826766, Philadelphia, PA 19182-6766

5. USE OF LICENSED PREMISES: Licensee covenants and agrees that it shall use the Licensed Premises, exclusively, to provide a program of individual and group counseling services for domestic violence offenders through its Abuser Intervention Program at the Licensed Premises which services are further described in the Contract (the “Permitted Use”). Licensee agrees to ensure compliance with all licensing and operational requirements, and other federal, state and local laws regulating its use of the Licensed Premises. Licensee shall be responsible for obtaining all licenses and certifications required by State, Federal, and County law to operate the program as defined in the Contract. Failure to obtain and maintain any required certifications and licenses will constitute a breach of this License. Licensee will not use or occupy the Licensed Premises for any purpose other than the Permitted Use.

0

6. ASSIGNMENT: The Licensee shall not assign, transfer, mortgage or otherwise encumber this License or sublet or rent (or permit a third party to occupy or use) the Licensed Premises or any part of the Licensed Premises.

7. CONDITION OF LICENSED PREMISES: Licensee is in possession of the Licensed Premises and accepts the Licensed Premises in "as is" condition. Licensee agrees to maintain the Licensed Premises in good condition and free of clutter throughout the License Term. Licensee acknowledges and agrees that at the end termination or earlier expiration of the License Term, it will surrender the Licensed Premises to the County in the same condition as when Licensee accepted the Licensed Premises, with reasonable wear and tear and damage due to casualty excepted.

8. ALTERATIONS AND IMPROVEMENTS:

A. Licensee shall not undertake any alterations, changes or improvements to the Licensed Premises without the prior written consent of the County. In the event the County grants such consent, Licensee shall be responsible for the acquisition of any and all necessary permits and for the observance of all building and zoning ordinances and regulations then in effect and shall diligently pursue such approved alterations, changes or improvements. Failure to adhere to any previously approved plans, applicable ordinances or regulations shall be deemed to be a breach of this License.

B. Approval and Inspection: Approval of any alterations, changes or improvements to the Licensed Premises will be conditioned on Licensee submitting to the County plans and specifications clearly setting forth the work to be performed. The County shall respond in writing within forty-five (45) days from receipt of plans and specifications. The County shall inspect the premises upon completion of the work to determine adherence to submitted specifications and compliance with applicable codes and regulations. In the event that the completed work is not satisfactory to the County, Licensee shall undertake any necessary corrections, at Licensee's risk and expense.

C. Licensee expressly acknowledges that at the County's election, all alterations, installations, changes, replacements, additions to or improvements upon the Licensed Premises shall remain upon the Licensed Premises and be surrendered with the Licensed Premises at the expiration or earlier termination of this License without disturbance, molestation or injury. Alternatively, the County may require that all such

alterations, installations, changes, replacements, additions to or improvements upon the Licensed Premises be removed by Licensee at the expiration or earlier termination of this License, in which event Licensee hereby agrees to cause them to be removed at Licensee's sole cost and expense and to repair any damage caused by such removal, and, further, should Licensee fail to remove them, then in such event the County shall cause them to be removed at Licensee's expense, and Licensee hereby agrees to reimburse the County, as appropriate, for the cost of such removal together with any and all damages which County may suffer and sustain by reason on Licensee's failure to remove them.

9. LIENS: Licensee shall not do or suffer anything to be done whereby the Licensed Premises shall be encumbered by any lien, including mechanic's liens. Licensee expressly covenants and agrees that it will, within sixty (60) days after the filing thereof, promptly remove or release, by the posting of a bond or otherwise, as required or permitted by law, any lien attached to or upon the Licensed Premises or any portion thereof by reason of or any act or omission on the part of Licensee, and hereby expressly agrees to save and hold harmless the County from and against any such lien or claim of lien. In the event any such lien does attach, or any claim of lien is made against the Licensed Premises, and shall not be thus released within said sixty (60) day period, the County, in its sole discretion (but nothing herein contained shall be construed as requiring it so to do), may pay and discharge said lien and relieve the Licensed Premises from any such lien, and Licensee agrees to pay and reimburse the County immediately upon demand for or on account of any expense which may be incurred in discharging such lien or claim.

10. SERVICES AND OPERATING EXPENSES:

A. By County: Subject to and contingent upon annual appropriation by the County Council and except for work necessitated by reason of Licensee's negligent or wrongful act, the County agrees to provide within the Licensed Premises, at the County's sole cost and expense the services listed below. All such services shall be provided and performed at the same level and manner as provided and performed for all similar Montgomery County serviced properties.

- i. Maintenance of the fire alarm and security systems.
- ii. Repair, replacement and preventive maintenance of mechanical (including the elevators), HVAC, electrical and plumbing systems.

- iii. Major structural repairs.
- iv. Maintenance and repair to the exterior of the building envelope components including painting, roofing, waterproofing, and gutters, including gutter cleaning.
- v. Fire extinguisher service, inspections, and replacements as necessary.
- vi. Exterior painting as needed or as required by the County. Specifications of type of paint and colors shall be provided by the County. The County, at its own cost and expense, shall use its own contractor to complete the painting.
- vii. All custodial, janitorial and recycling services in the Licensed Premises, including the bathrooms (if any). Proper routine maintenance and repair (i.e. cleaning, waxing, sealing, shampooing) of all flooring products (i.e. luxury vinyl tile, VCT, porcelain tile, carpet, sealed concrete, etc.). General maintenance including but not limited to interior window cleaning, light bulb replacement; and maintenance required for code compliance. Trash removal, recycling and pest control

B. By Licensee: Licensee agrees to provide within the Licensed - Premises, at Licensee's sole cost and expense the services set forth below.

- i. Licensee will keep the License Premises in a neat and orderly manner and free of clutter
- ii Telephone and internet service, if needed is provided by Licensee.
- iii The Licensee shall maintain, repair and/or replace all kitchen appliances, if applicable. Such appliances include but are not limited to the following: refrigerators, freezers, hood systems, ovens, stovetops/ranges, microwaves, dishwashers, etc.
- iv. Any proprietary systems (i.e. computer systems, phone systems) are at the sole responsibility and cost of the Licensee.
- v. If a grease interceptor is required by governmental law to operate the kitchen, Licensee at its sole cost shall perform all applicable routine maintenance and repair of this equipment. (If applicable).

- vi. Appliance replacement when, in County's sole judgment, replacement is necessary due to abuse, misuse, deterioration, or negligence on the part of Licensee, its contractors, employees, patrons or agents. All appliances shall be approved by the County prior to their installation. Licensee must apply, if available, for any warranties for new appliances acquired for the facility and shall assign its rights under such warranties to County as the expiration or earlier termination of this License.
- viii. Licensee shall not proceed with or use any unusual or hazardous materials in the performance of these requirements without consent of the County.
- ix. Notwithstanding the obligations of the County regarding certain maintenance, Licensee will be responsible for damage to the interior of the structure, or contents of the Licensed Premises due to the willful or negligent acts of Licensee, Licensee's employees, patrons, invitees, clients, residents, or agents. In the event of such damage, the Licensee shall immediately make the necessary repairs or replacement to the satisfaction of the County at Licensee's sole cost and expense, or the County shall make such repairs or replacements for which Licensee shall promptly reimburse the County.

A summary of such repairs shall be transmitted quarterly to the Department of General Services, Office of Real Estate, 101 Monroe Street, 9th Floor, Rockville, Maryland 20850, Attention: Director of Real Estate.

11. FURNITURE, FIXTURES AND EQUIPMENT: At the termination of this License, Licensee must deliver to the County the Licensed Premises in good, clean condition, reasonable wear and tear excepted. All items which are attached to the Licensed Premises or are a part of the Licensed Premises systems at the time the Licensed Premises is delivered to Licensee, shall remain with the Licensed Premises. Any personal property remaining within the Licensed Premises after termination of the License shall be considered abandoned and become property of the County. The County shall dispose of any such property in the manner it deems appropriate and the Licensee agrees to reimburse the County immediately upon request for all costs and expenses incurred by the County in storing and/or disposing of said property.

12. LIABILITY, PROPERTY DAMAGE AND FIRE INSURANCE:

A. Insurance Requirements:

i. Licensee agrees to obtain and maintain, during the full term of this License, and any extension thereof, a policy of general liability insurance with a minimum limit of liability of Two Million Dollars (\$2,000,000) per occurrence and Five Million Dollars (\$5,000,000) for bodily injury and property damage including Contractual Liability, Premises and Operations, Independent Contractors, Personal Injury and fire legal liability issued by an insurance company licensed in the State of Maryland and acceptable to the County.

ii. Licensee agrees to obtain and maintain, during the full term of this License, a policy of workers' compensation and employers' liability meeting all statutory requirements of the State of Maryland with the following minimum Employers' Liability limits; *Bodily Injury by Accident - \$100,000 each accident, Bodily Injury by Disease - \$500,000 policy limits and Bodily Injury by Disease - \$100,000 each employee*

iii. Licensee agrees to obtain and maintain, an All-Risks Property Policy during the License term and any renewal terms to protect the full replacement value of all contents of the Licensed Premises and all business personal property and interests of the Licensee, the County and the Property of Others against any loss. Any deductibles under this policy shall be funded by the Licensee. The County does not provide any coverage for Licensee's owned contents, business personal property and improvements to the Licensed Premises. County shall be named as a loss payee as pertains to its interest in the improvements.

B. Additional Insured: The Licensee's Liability Policies must list Montgomery County, Maryland as an additional insured and all insurance policies obtained by the Licensee as required by this License Agreement must provide that the Licensee will give the County written notice of amendment, cancellation, termination or non-renewal, no later than forty-five (45) days prior to amendment, cancellation, termination or non-renewal. The Licensee must provide on an annual basis evidence that is satisfactory to the County of the insurance coverages required under this License Agreement and if requested copies of policies.

C. Certificate of Insurance: The Licensee must, within thirty (30) days from execution of this License Agreement, deliver to the County a certificate(s) of insurance and copy of policies evidencing the coverages required under this License Agreement. The certificates must be issued to: Montgomery County, Maryland, Department of General Services, Office of Real Estate, 101 Monroe Street, 9th Floor, Rockville, Maryland 20850. Licensee has the obligation to assure that the County always has a valid Certificate of Insurance and complete copies of the policies.

D. Subrogation: If a casualty or other occurrence which should be covered by the insurance required by this License Agreement occurs, the Licensee must look solely to its insurer for reimbursement and the Licensee must ensure that such insurance is so written that the Licensee's insurer waives all rights of subrogation and shall have no cause of action against the County, its agents, or employees as a result of such casualty or occurrence. The Licensee waives and releases all right of recovery which it might otherwise have against the County or its agents or employees by reason of any loss or damage resulting from such casualty or other occurrence.

E. County's Insurance: The County will maintain its normal fire and liability insurance on the Licensed Premises for its operations. The County reserves the right to self-insure.

13. HOLD HARMLESS. Licensee agrees to indemnify, hold harmless and defend the County, or at the County's sole option pay for the defense of the County, from any and all claims of liability, actions, damages and expenses, including, but not limited to, reasonable attorneys' fees and litigation costs, arising out of or related to Licensee's use of possession of the Licensed Premises and improvements appurtenant thereto at the Building and Licensed Premises, from any breach of this License by Licensee, or from any claim, action, damage, liability or expense occasioned wholly or in part by any negligent act, errors or omission of Licensee, its agents, contractors, guests, invitees, or employees, except such negligence as may be occasioned by the acts or omissions of the County, the County's employees, agents and contractors. Licensee further specifically agrees to hold the County harmless from and defend the County, or at the County's sole option pay for

the defense of the County, for any claim of liability made in connection with any construction, alteration, or improvement by Licensee to the Licensed Premises, whether or not approved by the County, or the installation of any equipment by the Licensee within the Licensed Premises.

14. RESPONSIBILITIES OF LICENSEE: Licensee covenants and agrees as follows:

A. Licensee shall not keep gasoline or other flammable material or any explosive within the Licensed Premises which will increase the rate of fire insurance on the Licensed Premises, Building or property beyond the ordinary risk established for the type of operations described in Paragraph 5, above. Any such increase in the insurance rate due to the above, or due to Licensee's operations within the Licensed Premises, shall be borne by Licensee. Licensee shall not willfully do any act or thing in or about the Licensed Premises which may make void or voidable any insurance on the Licensed Premises, Building or Property, and Licensee, upon receipt of the same in writing, agrees to conform to all rules and regulations established from time to time by the County, the Maryland Insurance Rating Bureau, or any other authority having jurisdiction over such matters.

B. Licensee shall not use or allow the Licensed Premises or any part thereof to be used for any illegal, unlawful or improper purpose or for any act or thing that may be a nuisance, annoyance, inconvenience, or cause damage to the Licensed Premises, adjacent properties or the adjacent neighborhood.

C. Licensee shall not place upon the Licensed Premises any placard, sign, lettering or awning except such, and in such place and manner as shall have been first approved in writing by County. However, at the Licensee's sole cost and expense, the Licensee shall be required to place upon the Licensed Premises signage prohibiting smoking or vaping of any kind in and around the Licensed Premises.

D. Licensee acknowledges that all responsibilities of Licensee relating to the use or misuse of the Licensed Premises and anything therein shall be construed to include use or misuse thereof by Licensee's agents, employees, guests and invitees.

E. Licensee shall not have animals in or about the Licensed Premises. This provision does not limit Licensee or Licensee's clients' rights to have bona fide service animals on the Licensed Premises. Licensee is solely responsible for the proper care of service animals in the Licensed Premises and in keeping the Licensed Premises clean and free of debris, waste and damage associated with the care and feeding of service animals.

F. Licensee, upon receipt of the same in writing shall comply with all reasonable rules and regulations with regard to the use of the Licensed Premises that may be from time to time promulgated by County, and any violation of said rules and regulations upon the expiration of any applicable notice and cure period shall be deemed to constitute a violation of this License. It is understood that such rules and regulations shall not unreasonably interfere with or prevent the intended uses of the Licensed Premises as set forth in this License. County shall not discriminate against Licensee in the enforcement of any rule or regulation. If there shall be a conflict between this License and rules and regulations, the terms of this License shall govern.

G. Licensee must maintain in good condition, and promptly and diligently repair any damage to (or replace if reasonably necessary in the circumstances), any trade fixtures.

H. Licensee must require and assure that all entrance doors and windows in the Licensed Premises shall be closed and locked when the Licensed Premises are not in use. Further, Licensee before closing and leaving the Licensed Premises at any time must close all windows and doors and secure the Licensed Premises. No additional locks or bolts of any kind shall be placed upon any of the entrance or interior doors or windows by Licensee nor shall any changes be made in existing locks or the mechanisms thereof without prior written approval of County, and in the event of an approved change shall provide County with keys to the facility. Licensee shall, upon the termination of this License, return to the County all keys associated with the Licensed Premises, whether furnished to, or otherwise procured by, the Licensee, and in the event of the loss of any keys so furnished the Licensee shall pay to the County the replacement cost thereof

I. Licensee must inform all occupants of the Licensed Premises as to all rules and regulations regarding the Licensed Premises established by the County and the safe and proper operation of all appliances and equipment in the Licensed Premises.

J. The Licensee must not strip, overload, damage, or deface the Licensed Premises or any part of the premises of which the Licensed Premises are a part, including, but not limited to, hallways, stairways, or elevators.

K. The Licensee must not permit any trade or occupation to be carried on or use made of the Licensed Premises outside the scope of this License. Further the Licensee agrees to and must obey any and all federal, state, county and local laws and regulations relating to its use of the Licensed Premises.

L The Licensee must not move any furniture or equipment which is the property of the County into or out of the Licensed Premises without the County's prior written consent.

15. DESTRUCTION OF LICENSED PREMISES: The County will have no obligations to restore the building or licensed premises and will have no liability to the licensee in the event of damage or destruction to the building or licensed premises' intention.

16. DEFAULT: Licensee shall be considered in default of this License and the County may terminate this License upon the occurrence of any of the following:

- i. Failure to perform under any term, covenant or condition of this License.
- ii. The commencement of any action or proceeding for the dissolution or liquidation of Licensee, or for the appointment of a receiver or trustee of Licensee's property.
- iii. The making of any assignment of this License or the Licensed Premises for the benefit of Licensee's creditors.
- iv. The abandonment of the Licensed Premises by Licensee.
- v. Any default or breach of the terms and conditions of this License.
- vi. Use of the Licensed Premises by the Licensee or with the consent of Licensee, for uses other than the Permitted Use set forth in Section 5 of this License; or
- vii. The intentional use of the Licensed Premises by Licensee or by Licensee's agents, employee, contractors, or guests, for any unlawful purpose.

17. ACCESS: County and its respective agents and employees shall have the right at all reasonable times, upon reasonable notice to the Licensee, to enter upon the Licensed Premises for the purpose of inspecting same, making necessary repairs, and showing same to potential purchases and mortgage lenders, and, during the last six (6) months of the License Term, to prospective tenants, with reasonable efforts to minimize interference or disruption to the Licensee.

18. SURRENDER OF POSSESSION: Licensee covenants and agrees that at the expiration or other termination of this License, it shall remove all goods and effects from the Licensed Premises not the property of County, and return to County the Licensed Premises and all keys, locks and other fixtures connected therewith (except property belonging to Licensee), in good repair, order and condition in all respects, reasonable wear and tear excepted and the use thereof and damage by fire or other casualty and damage from any risk with respect to which Licensee is not herein expressly made liable excepted. Licensee shall pay for all damages due to any waste, misuse, or neglect of said Licensed Premises, its fixtures, and appurtenances, by said Licensee, its agents, employees, guests or invitees.

19. NOTICE OF ACCIDENTS, DEFECTS OR DAMAGES: Licensee shall give to the County prompt verbal notice of accidents in or damages to the Licensed Premises, and, within twenty-four (24) hours, the Licensee shall follow-up with a detailed written report of such accidents or damages. Licensee shall provide notice by contacting the County's Division of Facilities Management-Customer Service number at 240-777-7777. This number can be used 24 hours/7 days per week.

20. COMPLIANCE WITH LAWS: It is understood, agreed and covenanted by and between the Parties that Licensee, at Licensee's expense, shall promptly comply with, observe and perform all of the requirements of all of the statutes, ordinances, rules, orders and regulations now in effect or hereinafter promulgated whether required by the Federal Government, State of Maryland, Montgomery County Government, or any municipality in which the Licensed Premises are located, Montgomery County Department of Environmental Protection or Montgomery County Fire Marshal's Office (the "Applicable Laws"). In no event shall Licensee be liable for any violations of Applicable Laws with respect to the Licensed Premises which are existing as of the Commencement Date.

21. WAIVER: The waiver at any time by either of the Parties of any particular covenant, condition, obligation, or duty under this License shall extend to the particular case only, and for the particular time and in the particular manner specified, and such waiver must not be construed or understood as waiving any further or other rights of either Party.

22. NON-DISCRIMINATION: The Licensee agrees to comply with the non-discrimination policies in County contracts as required by Section 11B-33 and Chapter 27 of the Montgomery County Code (2014), as amended, as well as all other federal, state and local laws and regulations regarding discrimination. By signing this License Agreement, the Licensee assures the County that in accordance with applicable law, it does not, and agrees that it will not engage in any discrimination in violation of the above sections of the Montgomery County Code as well as any other federal, state or local laws, rules and regulations.

23. PUBLIC EMPLOYMENT: The Licensee understands and agrees that unless authorized under Sections 11B-52 and Chapter 19A of the Montgomery County Code 2014, as amended, that it is unlawful for any person or entity transacting business contemporaneous with his or her public employment.

24. MAILING NOTICES: All notices required or desired to be given hereunder by either party to the other shall be given by certified or registered mail and shall be deemed to be effective when received or refused by the addressee. Notices to the respective Parties shall be addressed as follows:

Licensee:

The Baltimore Therapy Center, LLC
103 Old Court Road, Suite A
Baltimore, Maryland 21208
Attn: Raffi Bilek

County:

Montgomery County, Maryland
Department of General Services
Office of Real Estate
101 Monroe Street, 9th Floor
Rockville, Maryland 20850
Attn: Director of Real Estate

With a copy, that does not constitute Notice to:

Baltimore Therapy Center
8818 Georgia Avenue

Montgomery County, Maryland
Office of the County Attorney
101 Monroe Street, 3rd Floor
Rockville, Maryland 20850
Attn: County Attorney

25. RESIDENT AGENT: The Resident Agent for the Licensee is Raffi Bilek: Old Court Road, Suite A, Baltimore, MD 21208. Licensee must immediately notify County of any change in resident agent or address as provided herein.

26. PROHIBITION OF HAZARDOUS SUBSTANCES: Licensee will not use or permit the Licensed Premises to be used in violation of any Environmental Laws, nor will it use, generate, release, store, treat, dispose of, or otherwise deposit, in, on, or about the Licensed Premised and Building any Hazardous Substances, nor will it permit or allow any third party to do so without the County's prior written consent. The foregoing shall not preclude Licensee from using materials commonly used in the course of performing the Permitted Use, provided that Licensee properly handles and disposes of the same in accordance with applicable law and the manufacturers' instructions with respect thereto. The Licensee agrees not to store or bring hazardous substances onto the Licensed Premises. The term "hazardous substances" shall mean any substance, chemical, waste, product or the like which now or in the future is identified as hazardous, toxic, dangerous or the like, or is regulated or otherwise subject to any Environmental Laws, including, but not limited to, asbestos, polychlorinated biphenyls, urea formaldehyde insulation, and any substance which requires reporting, registration, notification, removal, abatement or special treatment, storage, handling or disposal under any Environmental Laws. The term "Environmental Laws" shall mean all existing and future Federal, state and local laws, regulations, ordinances and the like relating to the environment, as amended from time to time. Environmental Laws currently include, but are not limited to, the following: The Resource Conservation and Recovery Act of 1976 (42 U.S.C. §§6901 et. seq.) ("RCRA"), the Comprehensive Environmental Response, Compensation and Liability Act of 1980 (42 U.S.C. §§9601 et. seq.) ("CERCLA"), the Emergency Planning and Community Right to Know Act of 1986 (42 U.S.C. §§11001, et. seq.) ("EPCRA"), the Occupational Safety and Health Act of 1970 (29 U.S.C. §§651 et. seq.) ("OSHA") and the Toxic Substances Control Act (15 U.S.C. §§2601 et. seq.) ("TSCA"). The Licensee indemnifies the County against any and all claims of any personal injuries or personal and real property damage as a result

of any hazardous substance being brought on the Licensed Premises by the Licensee, its agents, contractors or employees or guests.

27. NON-APPROPRIATION: This License shall terminate automatically on July 1 of any year for which the County, for whatever reason does not appropriate funds to pay for the services specified in this License or its obligations under the Contract. The Licensee shall not make or be entitled to any claim for reimbursement of any kind, whether for improvements or prepaid items.

28. AMERICAN DISABILITIES ACT REQUIREMENTS: Licensee agrees that any future modifications it shall make to the Licensed Premises shall be made in conformance with the requirements of the Americans with Disabilities Act, the Federal Fair Housing Act, and all safety and accessibility requirements in Federal, State, and County Laws and regulations. Licensee must obtain all required permits prior to making any modifications to the Licensed Premises and must comply with all applicable building and safety codes.

29. EMINENT DOMAIN: The Licensee is not entitled to any condemnation award granted to the County as owner of the Licensed Premises. In the event that the Licensed Premises shall be taken by any governmental or quasi-governmental authority pursuant to its power of eminent domain or sold under threat of such taking, the Licensee will not be entitled to recover from the County any capital expenditures for improvements and betterments made by the Licensee to the Licensed Premises at the Licensee's expense.

30. FORCE MAJEURE: Neither Party will be deemed in default with respect to the performance of any terms, covenants, and conditions of this License if same shall be due to any strike, lockout, civil commotion, war-like operation, invasion, rebellion, hostilities, military or upsurged power, sabotage, inability to obtain any material or service, through natural or other cause beyond the control of either party; provided, however, that this provision shall not excuse any non-payment of License Fees. For purposes of this provision, lack of funds shall not be considered a cause beyond the control of a Party.

31. ENTIRE AGREEMENT: This License (which contains and includes the Exhibits) is the entire agreement between the Parties, and no representations, inducements, or agreement, oral or otherwise, between the Parties not contained in this License shall be of any force or effect.

32. MODIFICATION: This License (other than the Rules and Regulations, which may be changed from time to time) must not be modified in any manner except by an instrument in writing executed by both Parties with the same formality as this License.

33. GOVERNING LAW: This License and its performance is to be governed, interpreted, construed and regulated by the laws of Montgomery County and the State of Maryland.

34. CLAIMS: Any action brought by or on behalf of either Party in connection with the performance of this License must be filed and maintained in a court of competent jurisdiction in Montgomery County, Maryland. The Parties hereby waive their right to a trial by jury in any legal action relating to this License.

35. HOLDOVER: Upon the expiration or earlier termination of this License, Licensee shall peaceably surrender the Licensed Premises to the County in broom clean condition and good repair. In the event the Licensee remains in possession of the Licensed Premises at the expiration or earlier termination of the License, except with the express written consent of the County, Licensee shall be liable to and shall indemnify, defend and hold harmless the County from any and all damages alleged and/or sustained against it as a result of such holdover.

36. NO TENANCY CREATED: The Parties agree that this License Agreement is not intended to nor does it create a landlord/tenant relationship between LICENSEE and the County. LICENSEE acknowledges that the License granted by the County is for LICENSEE'S convenience only and is not a grant of any real property interest or tenancy, notwithstanding the requirement to maintain liability insurance or any other provision in this License Agreement to the contrary. Licensee agrees that the occupancy permitted by the County under this License Agreement does not convey to the LICENSEE any tenant rights or permit LICENSEE to avail itself of any landlord/tenant remedies permitted under the law.

SIGNATURE PAGE FOLLOWS

IN WITNESS WHEREOF, the Parties have caused this agreement to be properly executed.

WITNESS:

COUNTY
MONTGOMERY COUNTY,
MARYLAND

By: Gregory J Ossont
Greg Ossont, Deputy Director, General Services

By: Fariba Kassiri
Fariba Kassiri, Deputy Chief Administrative Officer

Date: 10/5/21

LICENSEE:
THE BALTIMORE THERAPY
CENTER, LLC.

By: myse

Date: 9/9/21

APPROVED AS TO FORM &
LEGALITY OFFICE OF THE
COUNTY ATTORNEY

RECOMMENDED

By: Neal Anker
Neal Anker
Associate County Attorney

By: Cynthia Brenneman
Cynthia Brenneman, Director
Office of Real Estate

Date: 10/4/2021

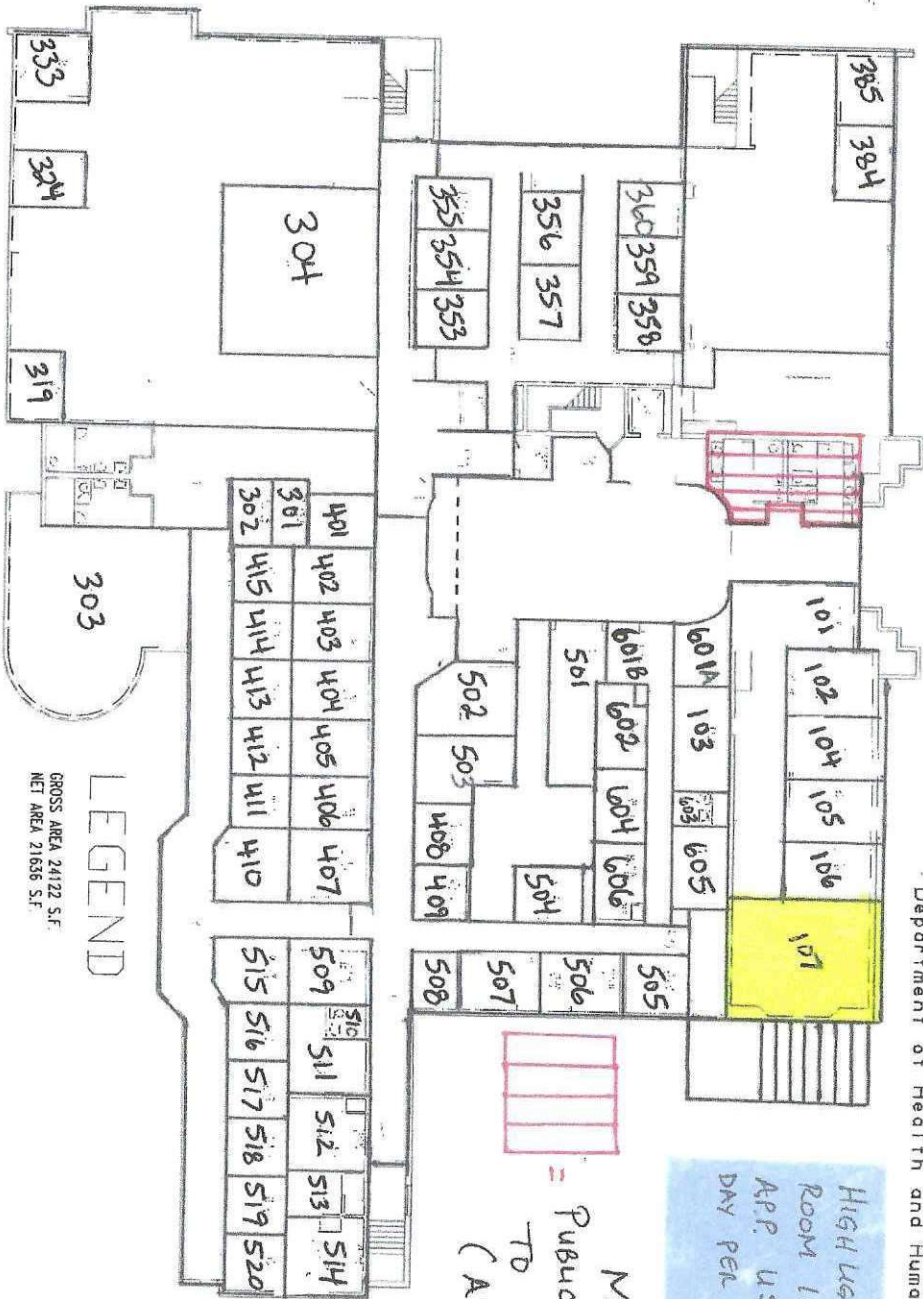
Date: 9/30/2021

EXHIBIT A
Leased Premises

Exhibit B

Contract

Silver Spring Regional Center
 8818 Georgia Avenue - 1st floor
 Montgomery County Maryland
 Department of Health and Human Services




LEGEND
 GROSS AREA 24122 S.F.
 NET AREA 21636 S.F.

HIGHLIGHTED
 ROOM 107 FOR
 APP. USE ONE
 DAY PER WEEK.

M/W
 = PUBLIC BATHROOMS
 TO BE REMODELED
 (ADA COMPLIANT)

Yes
 Grand's
 will send
 schedule

Silver Spring Regional Center
 8818 Georgia Avenue 2nd floor
 Montgomery County Maryland
 Department of Health and Human Services

 = M/W
 Public Bathrooms
 TO BE REMODELED
 (ADA COMPLIANT)



CONTRACT
1110701

This Contract is between Montgomery County, Maryland (the "County") and The Baltimore Therapy Center, LLC (the "Contractor"), located at 103 Old Court Road, Suite A, Baltimore, Maryland 21208.

BACKGROUND

1. The County wishes to provide a program of individual and group counseling services for domestic violence offenders through its Abuser Intervention Program. This program follows the Maryland State Operational Guidelines for Abuser Intervention Programs <http://goccp.maryland.gov/victims/family-violence-council/abuse-intervention>. Clients may voluntarily participate in these services or these services may be mandated for a client by the judicial system.
2. The County issued Request for Proposals # 1110701, Counseling Services for Domestic Violence Offenders on January 30, 2020 and issued Solicitation Amendment # 1 on February 28, 2020 and Solicitation Amendment # 2 on March 3, 2020.
3. The Contractor represents that it has the qualifications and experience to provide the services described in this Contract.
4. This Contract is entered into as a result of Request for Proposals # 1110701, Counseling Services for Domestic Violence Offenders inclusive of Solicitation Amendments # 1 and # 2.

ARTICLE I. SCOPE OF SERVICES

A. Abuser Intervention Program

- (1) The Contractor must provide counseling services for domestic violence offenders. Voluntary and court-ordered clients will be referred to the Contractor by the County. In most cases the Contractor will perform an assessment of clients prior to referral to the groups, although in some cases the County may refer a client without performing an assessment. The County will maintain the formal monitoring and communication with the courts and other referral agencies for mandated clients served under this Contract. The Contractor must collaborate with the County's Contract Monitor regarding the status of clients. The Contractor must provide services to clients within eight (8) business days after the client assessment has occurred. The ability to serve clients with English and Spanish languages is required, although other languages may also be required from time to time.
- (2) The Contractor must provide counseling services in accordance with State and County guidelines, including the Maryland State Operational Guidelines for Abuser Intervention Programs <http://goccp.maryland.gov/victims/family-violence-council/abuse-intervention> and the Maryland Network Against Domestic Violence www.mnadv.org. These services must be ethnically and culturally sensitive and must be offered on a flexible schedule.
- (3) The Contractor must provide the domestic violence offender counseling services described below according to models developed by, developed with, or approved by the County.

- (a) ***Clinical intake/assessment services (including victim partner contact):*** The Contractor must complete intake assessments by following the County's program procedures and forms which may include an automated intake system and paper forms. The intake must include completion of a biopsychosocial assessment which contains all relevant facts from relevant sources relating to the individual client's domestic violence offenses, the degree and length of the domestic abuse problem, relationship history and family dynamics, appropriate victim/partner contacts, presence of mental health and/or substance use disorder symptoms or conditions, and other relevant information that directly affects the client. The clinical intake typically takes one and one-half hours (90 minutes) for the interview and one half-hour (30 minutes) to complete the paperwork. The assessment is subject to County review and approval.
- (b) ***Group counseling:*** The Contractor must provide group counseling using a curriculum provided by the County. The group counseling sessions must seek to educate and increase awareness about abuse, its illegality, and effects; address family histories and patterns; examine attitudes that lead to abusive behavior and assist clients to identify power and control issues in intimate relationships.

The Contractor must use cognitive-behavioral skill-building sessions, stages of change theory and motivational interviewing strategies to support cessation of abusive behavior and improve communication, self-care, and the development of empathy. The current group model is a 22-session series totaling 33 hours, which meets State of Maryland standards. Six (6) of these 22 sessions are described below in item "d", Short Term Group Counseling, and occur prior to the other sixteen (16) sessions described herein. The Contractor must make a good faith effort to have healthy size groups of 8 to 12 members to foster interactions amongst the clients. The Contractor must limit each group counseling session to a maximum of 12 clients. Groups must be formed in an "open model" allowing for new clients to enter at any time. The Contractor will typically have two leaders providing group counseling. Group counseling is the predominant service model at this time and must be the major type of treatment provided to clients served under this Contract. Changes to the current model or uses of different models and structures for the counseling services may be considered with the County and decided upon with the ultimate approval of the County.

- (c) The Contractor may provide one individual counseling session to address crisis management which may not be able to be addressed in the group sessions. Additional individual sessions must be pre-approved by the County.
- (d) Short Term ***group counseling:*** The Contractor must provide 6-week psychoeducational group counseling sessions for clients awaiting trial on domestic violence charges. These sessions are once a week for ninety (90) minutes each. These sessions are also available for voluntary

participants who wish to complete the full 22 session program. This open group service must focus on coping skills and cognitive reframing, individualized crisis intervention and problem-solving attention with prepared topics for group intervention such as “time out”, healthy managing of separation and child visitation, resources and support for themselves, understanding the legal system, and stages of change utilizing motivational interviewing strategies. This service is intended to also engage the client for standard, longer-term domestic violence counseling whether as a mandated or voluntary participant. As with standard group counseling a curriculum/model has been developed by the County and must be used by the Contractor unless an alternative is developed with the County or approved by the County.

- (e) The Contractor must provide appropriate case management services for all clients as part of its service delivery to the client. This includes but is not limited to such functions as making and facilitating referrals to needed supplemental services, monitoring such referrals and services, and discussing fees and attendance problems in a therapeutic fashion.
- (4) The Contractor must:
 - (a) Designate a phone line for domestic violence offenders to call. The phone line must be answered by the intake manager who will explain to the client the required paperwork needed, fee collection policies, requirements for successful completion of the program and who will offer an intake appointment for the client to complete the intake paperwork. The Contractor may also receive referrals to the program by other means such as direct referrals from Criminal Justice agencies which may be received by phone or through e-mail. The Contractor must maintain a calendar of all intake appointments and share the calendar on a monthly basis with the County as part of the statistical reporting requirements for this Contract.
 - (b) Be available by telephone to clients in distress or in crisis during business hours and provide follow-up to after-hours crisis calls to the Contractor the next business day. The County's Crisis Center will provide crisis coverage after normal County business hours for this program. The County employee(s) providing such coverage will take notes of any interaction with clients and will forward these notes to the County's Abused Persons Program. If the Contractor refers a client to the Crisis Center, the Contractor must consult with the Contract Monitor for the County's Abused Persons Program and, if necessary, with the Crisis Center to be clear about the situation and needs of the client. Counseling services must be provided to any individual in need of counseling sessions in response to any such crisis within two (2) business days of the emergency with the pre-approval of the County's Contract Monitor. The Contractor's Clinical Director must be available to respond to clients, their families, or their attorneys during regular business hours.

- (c) Provide counseling services during evening hours and on Saturdays at the two County provided locations to maximize client access to services.
 - (d) Operate the program in accordance with County's schedule for holidays and inclement weather/emergency closings. The holidays currently observed by the County include New Year's Day, Martin Luther King Jr.'s Birthday, Presidents Day, Memorial Day, Fourth of July, Labor Day, Veteran's Day, Thanksgiving Day, and Christmas Day. In the event of inclement weather or other emergency situations, the Contractor must follow the County's schedule for operation of the program. Prior to the commencement of services under this Contract, the Contractor must submit a proposed schedule for on-site services to the Contract Monitor. This schedule must address personnel schedules and schedules for group counseling services. Any changes to the proposed schedule must be submitted in writing to the Contract Monitor.
 - (5) The Contractor's supervisory and/or administrative staff must attend reasonably scheduled coordination or training meetings arranged by the County. At times, the Contractor's clinical staff may be expected to attend such meetings with the County, or the Contractor must arrange for information to be shared through the agency's supervisory staff and/or informational structures. The Contractor's group leaders and Clinical Director must attend the State's mandatory inter-personal violence training sessions when scheduled.
 - (6) The Contractor must make a good faith effort to inform the County of unsatisfactory termination and successful completion of counseling by a client within five business days. Prior to terminating a client from the program, the Contractor must consult with the County's Contract Monitor and must not terminate the client prior to receiving approval from the County's Contract Monitor. Notice will be according to the method established by the County, to include phone, fax, email, and appropriate forms.
 - (7) At the request of the County, the Contractor must provide consulting services on an as-needed basis for the County's Abused Persons Program and must provide qualified staff as approved by the County to participate in program and/or community planning efforts. As part of the required consulting services, the Contractor must share clinical experiences with the County's Abuse Persons Program staff and write reports as required by the County.
- B. Facilities/Equipment/Locations - The Contractor must provide the services referenced in this Contract in two locations provided to the Contractor by the County for this purpose. The Contractor must sign and comply with a space license agreement with the County's Department of General Services related to the use of the County space. When using County space for client services, the Contractor must oversee all clients and maintain facilities and equipment in accordance with terms of the space license agreement. The Contractor must purchase and secure all office supplies, materials, audiovisual equipment, videos, and other supplies required to provide counseling services, case record forms and office forms.

C. The Contractor must provide each client with the following information both in person and in writing upon the client's commencement of services with the Contractor:

- (1) Notice of Privacy Practices and Confidentiality Policy, which makes clear the ability of the Contractor to share information with the County's Abused Persons Program for clinical purposes in addition to administrative purpose of monitoring services provided under this Contract;
- (2) name and phone number of his or her counselor(s) and information about regular business hour contacts and crisis coverage;
- (3) times and locations of counseling sessions and other services if applicable;
- (4) requirements for successful compliance, attendance, and make-up sessions, including procedures and consequences of discontinuation or termination of services, especially for mandated clients;
- (6) for offender clients, the Contractor must provide each client's victim with information about the offender's compliance with the program as part of maintaining compliance with Maryland State Guidelines for Abuser Intervention Programs unless advised otherwise by the Contract Monitor:
<http://goccp.maryland.gov/victims/family-violence-council/abuse-intervention>
- (7) notice of Contractor's procedure for handling complaints and grievances, including clear identification of staff members (with contact information) within the Contractor's organization for handling complaints and grievances and the County staff member responsible when these procedures do not satisfactorily resolve the grievance.
- (8) Provide offenders with fee policy information and the individual assessment of the offender's fee for services.

D. Policies/Procedures

- (1) The Contractor, within ten (10) days of execution of the Contract, must meet with County representatives to plan for the Contractor's assumption of counseling services under this Contract. The Contractor must follow all applicable laws and regulations for the delivery of human services and psychotherapy.
- (2) The Contractor also must develop and implement, within ninety (90) days of Contract execution, a policy and procedure approved by the County for the orderly discharge of clients from services, including a plan for the orderly transfer and disposition of clients at time of discharge. Each problematic discharge (discharge due to non-compliant behavior or other situation) from service must be approved by the County. The Contractor must develop and implement a policy and procedure approved by the County for the orderly transfer or disposition of the Contractor's caseload of clients referred under the Contract upon termination of the Contract. This policy must address: the time period for the completion of the transfer or disposition of the Contractor's

caseload and the plan to assure that adequate client services are continued during the transition period. The Contractor must implement the policy and procedure for caseload transfer or disposition upon written notice from the County.

(3) Fee Collection Policy

- (a) The Contractor must collect fees for counseling services according to the County's current fee schedule and ability-to-pay scale for offender counseling services. The County will provide the then current fee schedule and ability-to-pay scale to the Contractor before Contract execution and at the start of each County fiscal year. The Contractor will credit the County on the monthly invoice for all fees collected from clients. The Contractor must submit a report with the monthly invoice detailing the fees collected each month, the names of the clients paying fees and the names of the clients who have been non-compliant in the payment of fees. The County is not responsible for the failure of the Contractor to collect client fees. The County may, in its discretion, utilize the fees collected from clients to expand the services under this Contract. Any additional services and compensation will be added via a written amendment to this Contract. Contractor must not perform any additional services without first receiving a written Purchase Order and Notice to Proceed from the County.
- (b) The Contractor must not deny services to clients who fail to pay fees. Client's failure to pay fees should be addressed clinically with clients regularly. If a client attends a minimum of two sessions without paying fees to the Contractor, the Group Leader should talk with the his/her supervisor for guidance on resolving the issue with the client. If the client fails to pay fees for four sessions, the case must be referred to the County for review, within one week, for a determination of whether the client should be terminated from the program. Uncollected fees are fees for services that a client received but did not pay for; the County is not responsible for any uncollected fees.
- (c) The Contractor must make a concerted effort to collect fees according to good business practices and in keeping with the program's philosophy of personal responsibility.
- (d) The Contractor must keep a cumulative record of the number of clients in attendance, the total amount of payments due from those clients, and the total amount of payments collected.

(4) Grievance Policy and Procedures

The Contractor must develop and implement a plan within sixty (60) days of the effective date of the Contract, to be approved by the County, to maintain an internal quality review system that includes monitoring of the customer satisfaction survey (administered at least at termination of services) and a mechanism for addressing customer complaints, resolving grievances of

consumers and employees, subcontractors and consultants and taking corrective action following serious incidents.

- (5) Contractor must provide policy and procedure to deliver services in facilities with attention to the safety of patrons/customers. Contract services to domestic violence offenders must not be delivered at the same time or in the same location where domestic violence victims are receiving services.
- (6) Additional Contractor Staffing Requirements

The Contractor must:

1. Provide sufficient office support functions (which may include discrete staff member(s)) to receive and communicate with clients, schedule intake appointments, collect fees and carry out necessary administrative support for delivering the counseling services, including assisting with reports, data, and correspondence. Office hours and clinical hours of operation must be regularly scheduled to include a combination of day and evening hours;
2. Ensure that all staff possess appropriate credentials and supervision arrangements to ensure confidentiality and privileged communication to provide clinical counseling services according to Maryland law;
3. Develop and implement a policy that staff employed by the Contractor must be violence free in their own lives in accordance with Maryland State Guidelines for Abuser Intervention Programs (AIP): <http://goccp.maryland.gov/victims/family-violence-council/abuse-intervention>;
4. Develop and implement a policy that staff employed by the Contractor for this program of services must not use alcohol or drugs to an extent or in a manner that is determined to impair the individual's ability to function in a responsible and professional manner;
5. Provide or arrange for training necessary for staff to meet the requirements to deliver the specified services including the State's mandatory inter-personal violence training and document the trainings;
6. Provide, upon a vacancy in the service provider/counseling staff, an appropriate replacement person having qualifications equal to or better than the qualifications of the person being replaced, at no additional cost to the County. The Contractor must provide this replacement as soon as feasible and provide the appropriate coverage with existing staff or subcontractors, to include but not limited to the utilization of the Clinical Director upon occurrence of

the vacancy. If the Contractor is unable to provide such coverage, it must immediately provide written notification of the situation to the County. The Contractor must also ensure that supervisory and administrative functions are provided regardless of vacancies in the supervisory/administrative staff;

7. Provide a staffing schedule which ensures appropriate availability for communication between the Contractor's supervisory, administrative, and clinical staff with clients and the County. The Clinical Director must provide both day and evening work hours on-site. The Clinical Director must be on-site and provide program oversight and supervision utilizing a combination of day and evening hours to support the group leaders.
 8. The Contractor must ensure that all staff assigned to this program are trained on applicable client confidentiality regulations, policies and procedures, maintain confidentiality of health services rendered to clients and of other client health information, and comply with the requirements of the federal Health Insurance Portability and Accountability Act (HIPAA) and state medical and psychotherapy record laws.
 9. The County's Abused Persons Program, with Contractor services, must be certified under the Family Violence Council's Operational Guidelines for Abuser Intervention Programs
<http://goccp.maryland.gov/victims/family-violence-council/abuse-intervention/>
- E. The Contractor and/or their subcontractors or consultants must comply with the DHHS Background Clearance policy requirements for staff, subcontractors, and volunteers serving clients (please see link for policy):
<http://www.montgomerycountymd.gov/HHS/DoingBuswDHHS.html>
- F. Behavioral Health and Crisis Services in DHHS has adopted the National Standards for Culturally and Linguistically Appropriate Service in Health and Health Care (CLAS). CLAS standards are a comprehensive series of guidelines that inform, guide and facilitate practices related to culturally and linguistically appropriate health services. The Contractor and its subcontractors/consultants must adhere to CLAS in the provision of services under the Contract. For more information about CLAS, please go to: <https://www.thinkculturalhealth.hhs.gov/clas>
- G. The Contractor and/or its subcontractors and consultants must comply with all federal, state and local laws and regulations governing privacy and the protection of health information. The Contractor must execute formal agreements with other service providers in accordance with federal and state confidentiality regulations and the Health Insurance Portability and Accountability Act or with appropriate release of information by the Client.
- H. The Contractor must sign and comply with the Business Associate Agreement which will be incorporated by reference and made a part of the Contract at Attachment C.

- I. The Contractor must comply with the County's quality assurance measures which include permitting the County to conduct on-site visits, chart reviews related to this Contract, and reviews or requests for other data related to this Contract including staff and subcontractors' personnel folders to include documented trainings. Any site visit would be conducted at a mutually agreeable date and time. The Contractor must grant the County access to these records during the Contract term and for five (5) years after final payment under this Contract. Additionally, the Contractor must allow the Contract Monitor to attend/observe group sessions at any time.
- J. 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). The County's Information Resources Security Procedure (AP 6-7) references the County Computer Security Guideline and the County's Administrative Procedure 6-1, Administrative Procedure 6-7 and 6-1 are incorporated by reference and made a part of this Contract as Attachment D.
- K. During the COVID-19 pandemic, the Contractor may be required to provide services remotely through telework, teleconference or teletherapy. The Contractor must provide these services in accordance with the County's plan for telework. Any changes to the Contractor's telework plan must be submitted in writing to the Contract Monitor. When providing in-person services during the COVID-19 pandemic the Contractor must follow all County government guidelines to include all recommended precautions to avoid the spread of the virus, including, but not limited to, use of face coverings, social distancing, and health checks of staff and clients.

ARTICLE II. RECORDS AND REPORTS

A. Records and Reports

- 1. The Contractor must maintain all client records according to the County's policy on confidentiality and in accordance with federal and state laws and regulations governing privacy and clinical psychotherapy services including the Maryland Network Against Domestic Violence, <https://mnadv.org/mnadvWeb/wp-content/uploads/2013/03/comar.pdf> governing domestic violence program records. All client records are considered the property of the County. Upon termination of client services, the Contractor must perform the following within 60 days: 1) complete all paper recording in client records including group and individual progress notes, termination summary forms, copies of any necessary correspondence; and 2) complete all automated system data entry, if needed. The Contractor must return completed and organized files to the County for the Contract Monitor's final review and filing.

2. The Contractor must submit to the County monthly statistical data reports for all intake appointments provided during the month, all clients served in the month, the services provided to each client, the fees charged to clients, and the fees collected from clients. The reports must be in a County-approved format (including electronic formats) and must be submitted by the **5th business day** of the following month.
3. The Contractor must provide a quarterly report detailing their progress towards meeting the Outcome and Performance Measures listed in Item A, below. This report must be submitted by the 5th business day following the end of the quarter.

ARTICLE III. OUTCOME AND PERFORMANCE MEASURES

A. OUTCOME AND PERFORMANCE MEASURES

The Contractor must engage in data collection as directed by the County and administer a client satisfaction survey to provide information for measuring outcomes. Outcome measures include:

1. client satisfaction rate: Goal--85% will report that services were "helpful" or "very helpful" on the satisfaction survey.
2. numbers of clients engaged and retained: the goal is 60% of offender clients assigned to ongoing services will successfully complete services.
3. cessation of partner abuse by offenders (measured by self-report): Goal-- 80% of offenders will report not having used physical abuse in the previous 6 months on a survey at termination of services; and
4. Cessation of partner abuse as reported by victims and/or court records as required by the Maryland State Guidelines for Abuser Intervention Programs guidelines.

ARTICLE IV. COMPENSATION

- A. The Contractor's fiscal year line item budget as approved by the County is incorporated by reference and made a part of this Contract as **Attachment B**. Modifications to the Contractor's approved budget during the fiscal year must be justified by the proposing party and must be approved in writing by the Program Monitor.
- B. The County will reimburse the Contractor for all costs incurred in providing the goods and services described in this Contract, subject to the following limitations:
 - 1. No compensation will be paid for any costs that exceed the relevant line item in the Contractor's Budget by more than 10%.
 - 2. No compensation will be paid for any costs that exceed the overall total of the Contractor's Budget for each fiscal year.
 - 3. No services shall be performed by the Contractor under this Contract prior to the execution of a County Purchase Order for those services, and the Contractor's receipt of the said County Purchase Order.
 - 4. Compensation must not exceed funds appropriated by the County and encumbered in the County Purchase Order issued to the Contractor.
 - 5. The maximum compensation for the initial term of this Contract must not exceed \$399,999.55.
- C. The Contractor must comply with Montgomery County's DHHS Allowable Contract Cost Reimbursement Policy, which can be found at:
<http://www.montgomerycountymd.gov/HHS/DoingBuswDHHS.html>.
- D. At the County's discretion, the client fees collected, as described in Article I, Scope of Services, Section D, Policies and Procedures, Item 3, Fee Collection Policy, Paragraph "a" may be used to expand the services provided under this Contract. Any additional services and compensation will be added via a written amendment to this Contract. Contractor must not perform any additional services without first receiving a written Purchase Order and Notice to Proceed from the County.

ARTICLE V. 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. Upon receipt, acceptance, and approval of the Contractor's invoice, the County will make payment, net 30 days, for expenses incurred by the Contractor in providing the goods and services described in this Contract. All required reports and other supporting documentation must be provided with the Contractor's monthly invoice. Invoices must be sent to the Program Monitor designated by the County.

ARTICLE VI. TERM

The effective date of this Contract begins upon signature by the Director, Office of Procurement and continues for a one-year term. The period in which Contractor must perform all work under the Contract begins on the Contract's effective date and ends one year following the effective date. Contractor must also perform all work in accordance with time periods stated in the Scope of Services. Before this term for performance ends, the Director at his/her sole option may (but is not required to) renew the term. The Contractor's satisfactory performance does not guarantee a renewal of the term. The Director may exercise this option to renew this term four (4) times(s) for one year each.

ARTICLE VII. GENERAL CONDITIONS AND INSURANCE

The General Conditions of Contract Between County and Contractor ("General Conditions") are incorporated by reference into and made a part of this Contract as Attachment A. The insurance requirements set forth below supersede the insurance requirements set forth in Provision 21 of the General Conditions.

MANDATORY MINIMUM INSURANCE REQUIREMENTS

Counseling Services to Domestic Violence Offenders - Intake Assessments, Group and Individual Counseling (their sites)

Prior to the execution of the contract by the County, the Contractor and their contractors (if requested by County) 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 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 Contractor to the County nor shall failure to request evidence of this insurance in any way be construed as a waiver of Contractor's obligation to provide the insurance coverage specified. The Contractor's insurance shall be primary. 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.

Commercial General Liability

A minimum limit of liability of **one million dollars (\$1,000,000), per occurrence and one million (\$1,000,000) aggregate**, 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
- Sexual Molestation and Abuse

Professional Liability (Errors and Omissions Liability)

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

Each Claim

\$1,000,000

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

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, automobile insurance, 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.

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, MD
HHS / CMT
401 Hungerford Drive, 6th floor
Rockville, Md 20850

ARTICLE VIII. PRIORITY OF DOCUMENTS


The following documents are incorporated by reference into and made a part of this Contract, and are listed in order of legal precedence below, in the event of a conflict in their terms:

1. This Contract Document;
2. The General Conditions of Contract Between County and Contractor (Attachment A);
3. Business Associate Agreement (Attachment C);
4. Contractor's Fiscal Year Line Item Budget (Attachment B); and
5. Administrative Procedure 6-7 and 6-1 (Attachment D).

SIGNATURE PAGE TO FOLLOW

SIGNATURES

THE BALTIMORE THERAPY
CENTER, LLC

By: 

Typed Name: Raffi Bilek

Title: Director, Baltimore Therapy Center

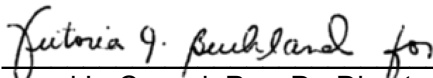
Date: 10/28/20

MONTGOMERY COUNTY, MARYLAND

By:  for
Avinash G. Shetty Director
Office of Procurement

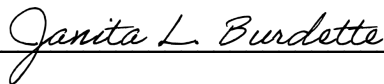
Date: 12/1/2020

RECOMMENDED

By:  for
Raymond L. Crowel, Psy. D., Director
Department of Health and Human Services

Date: 10/29/2020

APPROVED AS TO FORM & LEGALITY
OFFICE OF THE COUNTY ATTORNEY

By: 

Date: October 28, 2020

 11/19/2020
Chief, Division of Finance and
Procurement

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. 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 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;

Attachment A

- (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.

Attachment A

- 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)

Attachment A

	<u>Up to 50</u>	<u>Up to 100</u>	<u>Up to 1,000</u>	<u>1,000</u>
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
255 Rockville Pike, Suite 180
Rockville, Maryland 20850 4166

*Professional services contracts only

(Remainder of Page Intentionally Left Blank)

Attachment A

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

	<u>Up to 50</u>	<u>Up to 100</u>	<u>Up to 1,000</u>	<u>1,000</u>
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
255 Rockville Pike, Suite 180
Rockville, Maryland 20850 4166

(Remainder of Page Intentionally Left Blank)

Attachment A

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. 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.

Attachment A

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.

8.1.1.11: DHHS Contract Budget

Vendor/Organization Name:	The Baltimore Therapy Center, LLC
Address:	103 Old Court Rd. Suite A
City, State, Zip Code:	Baltimore, MD 21208
Contact Person:	Raffi Bilek
Phone/Fax/E-Mail:	443-273-4046
Contract Number:	1110701
Service Area:	HHS

BUDGET SUMMARY

	FY 2021 Budget
Category	Contract Expenses
A. Salary Expenses	\$303,600.32
Fringe Benefits (7.95% of salary expenses)	\$24,136.23
Total Personnel (Salary + Fringe)	\$327,736.55
B. Direct (Operating) Expenses	\$32,263.00
C. Capital Expenses	\$0.00
Subtotal of Contract Expenses	\$359,999.55
Indirect/Administration	\$40,000.00
Total Contract Budget:	\$399,999.55

BUDGET DETAIL

A. Salary Expenses and Fringe Benefits

Position	Incumbent	Annual Salary	Full Time equivalent (FTE), this contract	Expenses to this Contract	Fringe Benefit Rate	Fringe Benefits	Justification for Position
Clinical Director	Raffi Bilek, LCSW-C	\$85,000.00	1	\$ 85,000.00	7.95%	\$ 6,757.50	Manages all staff and programming.
Intake/outreach manager	Luzelenya Ramos, JD	\$48,000.00	1	\$ 48,000.00	7.95%	\$ 3,816.00	Coordinates intake schedule and administration, conducts victim outreach
Intake worker	Chantelle Prince, LMSW	\$57,000.00	1	\$ 57,000.00	7.95%	\$ 4,531.50	Conducts intakes in English.
Adminstrative assistant	Joyce Chapman	\$38,000.00	1	\$ 38,000.00	7.95%	\$ 3,021.00	Provides administrative support.

Group leader	Carlos Vera, LCSW	\$104,000.00	0.12	\$ 12,480.00	7.95%	\$ 992.16	Runs groups in English and Spanish.
Group leader	Marie Pasti, LCSW-C	\$77,156.00	0.12	\$ 9,258.72	7.95%	\$ 736.07	Runs groups in English.
Group leader	Soni Fitzhugh, LMSW	\$52,000.00	0.23	\$ 11,960.00	7.95%	\$ 950.82	Runs groups in English.
Group leader	Deneen Robin, LCPC	\$56,160.00	0.135	\$ 7,581.60	7.95%	\$ 602.74	Runs groups in English.
Group leader	Steven Rothman, LGPC	\$52,000.00	0.12	\$ 6,240.00	7.95%	\$ 496.08	Runs groups in English.
Group leader	Xiomara Medina, LGPC	\$93,600.00	0.3	\$ 28,080.00	7.95%	\$ 2,232.36	Runs groups and conducts intakes in Spanish.
Total Salary Expenses				\$ 303,600.32	Total Fringe	\$ 24,136.23	

B. Direct (Operating) Expenses

Expense Category		Cost	Justification of Costs				
Consulting (if more than one consultant, list each one on a separate line)		\$ -					
Staff Development		\$ 600.00	Required DV training for all staff - currently free, but this is not always true.				
Payroll		\$ 1,946.00					
Travel		\$ -					
Rent		\$ -					
Utilities		\$ -					
Maintenance		\$ -					
Telephone Bill		\$ -					
Other Communications		\$ -					
Equipment (up to \$5,000)*		\$ -					
Supplies		\$ 1,190.00	Based on estimates of supplies needed for programming, not administrative, purposes.				
Insurance		\$ 2,063.00	Quote provided by HPSO based on County's requirements.				
Postage		\$ 330.00	Estimated 600 letters to be sent out per year for intake clients.				
Printing		\$ 800.00	Based on estimates of number of pages printed per year, at an average cost of \$.06 per page.				
Other Expenses (list)		\$ -					
interpretation services		\$ 11,985.00	Based on estimate provided by UNO Tranlsation services for an average of 5 foreign-language clients per year (including victim contacts).				
background checks		\$ 649.00					
educational videos		\$ 200.00	Updated videos are badly needed for the program. Many of the ones we use are from the 1980s and 1990s.				
bookkeeping/accounting		\$ 12,000.00	Estimate provided by Gross, Mendelsohn & Associates				
staff recruiting		\$ 500.00					
Total Direct Expenses		\$ 32,263.00					

C. Capital Expenses, if applicable (greater than \$5,000)*

Description		Cost	Justification of Costs				
		\$ -					
		\$ -					
		\$ -					
Total Capital Expenses		\$ -					

Indirect Costs

Description		Cost	Justification of Costs
contractor fee		\$ 40,000.00	10% of contract budget
Total Indirect Costs		\$ 40,000.00	

Approved by: (for the Vendor)



9/30/2020

Signature

Date

Name (please print): Raffi BilekTitle: Director

Approved by: (Monitor, for the Dept. of Health and Human Services)



9/30/20

Signature

Date

Name (please print): Nadja S.P. CabelloTitle: Manager for Trauma Services: APP and VASAP

*Equipment includes items up to \$5,000. Items greater than \$5,000 are capital expenses.

ATTACHMENT C

BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement (the “Agreement”) is made by and between Montgomery County, Maryland (hereinafter referred to as “Covered Entity”), and The Baltimore Therapy Center, LLC (hereinafter referred to as “Business Associate”). Covered Entity and Business Associate shall collectively be known herein as the “Parties.”

I. GENERAL

A. Covered Entity has a business relationship with Business Associate that is memorialized in Montgomery County Contract # 1110701 (the “Underlying Agreement”), pursuant to which Business Associate may be considered a “business associate” of Covered Entity as defined in the Health Insurance Portability and Accountability Act of 1996, including all pertinent regulations (45 CFR Parts 160 and 164), issued by the U.S. Department of Health and Human Services, including Subtitle D of the Health Information Technology for Economic and Clinical Health Act (the “HITECH Act”), as codified in Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (Pub. L. 111–5), and including any and all applicable Privacy, Security, Enforcement, or Notice (Breach Notification) Rules or requirements (collectively, “HIPAA”), as all are amended from time to time; and

B. The performance of the Underlying Agreement may involve the creation, exchange, or maintenance of Protected Health Information (“PHI”) as that term is defined under HIPAA; and

C. For good and lawful consideration as set forth in the Underlying Agreement, Covered Entity and Business Associate enter into this Agreement for the purpose of ensuring compliance with the requirements of HIPAA; and

D. This Agreement articulates the obligations of the Parties as to use and disclosure of PHI. It does not affect Business Associate’s obligations to comply with the the Maryland Confidentiality of Medical Records Act (Md. Code Ann., Health-General I §§4-301 *et seq.*) (“MCMRA”) or other applicable law with respect to any information the County may disclose to Business Associate as part of Business Associate’s performance of the Underlying Agreement; and

E. This Agreement supersedes and replaces any and all Business Associate Agreements the Covered Entity and Business Associate may have entered into prior to the date hereof; and

F. The above premises having been considered and incorporated by reference into the sections below, the Parties, intending to be legally bound, agree as follows:

II. DEFINITIONS.

A. The terms used in this Agreement have the same meaning as the definitions of those terms in HIPAA. In the absence of a definition in HIPAA, the terms have their commonly understood meaning.

ATTACHMENT C

B. Consistent with HIPAA, and for ease of reference, the Parties expressly note the definitions of the following terms:

1. “Breach” is defined at 45 CFR § 164.402.
2. “Business Associate” is defined at 45 CFR § 160.103, and in reference to the party to this Agreement, shall mean The Baltimore Therapy Center, LLC
3. “Covered Entity” is defined at 45 CFR § 160.103, and in reference to the party to this Agreement, shall mean the County.
4. “Designated Record Set” is defined at 45 CFR § 164.501.
5. “Individual” is defined at 45 CFR §§ 160.103, 164.501 and 164.502(g), and includes a person who qualifies as a personal representative.
6. “Protected Health Information” or “PHI” is defined at 45 CFR § 160.103.
7. “Required By Law” is defined at 45 CFR § 164.103.
8. “Secretary” means the Secretary of the U.S. Department of Health and Human Services or designee.
9. “Security Incident” is defined at 45 CFR § 164.304.
10. “Unsecured Protected Health Information” or “Unsecured PHI” means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology, as specified by the Secretary in the guidance as noted under the HITECH Act, section 13402(h)(1) and (2) of Public Law 111-5, codified at 42 U.S.C. § 17932(h)(1) and (2), and as specified by the Secretary in 45 CFR 164.402.

III. PERMISSIBLE USE AND DISCLOSURE OF PHI

A. Except as otherwise limited in this Agreement, or by privilege, protection, or confidentiality under HIPAA, MCMRA, or other applicable law, Business Associate may use or disclose (including permitting acquisition or access to) PHI to perform applicable functions, activities, or services for, or on behalf of, Covered Entity as specified in the Underlying Agreement. Moreover, the provisions of HIPAA are expressly incorporated by reference into, and made a part of, this Agreement.

B. Business Associate may use or disclose (including permitting acquisition or access to) PHI only as permitted or required by this Agreement or as Required By Law.

C. Business Associate is directly responsible for full compliance with the relevant requirements of HIPAA.

ATTACHMENT C

D. Business Associate must not use or disclose (including permitting acquisition or access to) PHI other than as permitted or required by this Agreement or HIPAA, and must use or disclose PHI only in a manner consistent with HIPAA. As part of this, Business Associate must use appropriate safeguards to prevent use or disclosure of PHI that is not permitted by this Agreement or HIPAA. Furthermore, Business Associate must take reasonable precautions to protect PHI from loss, misuse, and unauthorized access, disclosure, alteration, and destruction.

E. Business Associate must implement and comply with administrative, physical, and technical safeguards governing the PHI, in a manner consistent with HIPAA, that reasonably and appropriately protect the confidentiality, integrity, and availability of the PHI that it creates, receives, maintains, or transmits on behalf of Covered Entity.

F. Business Associate must immediately notify Covered Entity, in a manner consistent with HIPAA, of: (i) any use or disclosure of PHI not provided for by this Agreement, including a Breach of PHI of which it knows or by exercise of reasonable diligence would have known, as required at 45 CFR §164.410; and, (ii) any Security Incident of which it becomes aware as required at 45 CFR §164.314(a)(2)(i)(C). Business Associate's notification to Covered Entity required by HIPAA and this Section III.F must:

1. Be made to Covered Entity without unreasonable delay and in no case later than 14 calendar days after Business Associate: a) knows, or by exercising reasonable diligence would have known, of a Breach, b) becomes aware of a Security Incident, or c) becomes aware of any use or disclosure of PHI not provided for by this Agreement;

2. Include the names and addresses of the Individual(s) whose PHI is the subject of a Breach, Security Incident, or use or disclosure of PHI not provided for by this Agreement. In addition, Business Associate must provide any additional information reasonably requested by Covered Entity for purposes of investigating the Breach, Security Incident, or use or disclosure of PHI not provided for by this Agreement;

3. Be in substantially the same form as Exhibit A hereto;

4. Include a brief description of what happened, including the date of the Breach, Security Incident, or use or disclosure of PHI not provided for by this Agreement, if known, and the date of the discovery of the Breach, Security Incident, or use or disclosure of PHI not provided for by this Agreement;

5. Include a description of the type(s) of Unsecured PHI that was involved in the Breach, Security Incident, or use or disclosure of PHI not provided for by this Agreement (such as full name, Social Security number, date of birth, home address, account number, disability code, or other types of information that were involved);

6. Identify the nature and extent of the PHI involved, including the type(s) of identifiers and the likelihood of re identification;

ATTACHMENT C

7. If known, identify the unauthorized person who used or accessed the PHI or to whom the disclosure was made;

8. Articulate any steps the affected Individual(s) should take to protect him or herself from potential harm resulting from the Breach, Security Incident, or use or disclosure of PHI not permitted by this Agreement;

9. State whether the PHI was actually acquired or viewed;

10. Provide a brief description of what the Covered Entity and the Business Associate are doing to investigate the Breach, Security Incident, or use or disclosure of PHI not provided for by this Agreement, to mitigate losses, and to protect against any further Breach, Security Incident, or use or disclosure of PHI not provided for by this Agreement;

11. Note contact information and procedures for an Individual(s) to ask questions or learn additional information, which must include a toll-free telephone number of Business Associate, along with an e-mail address, Web site, or postal address;

and

12. Include a draft letter for the Covered Entity to utilize, in the event Covered Entity elects, in its sole discretion, to notify the Individual(s) that his or her PHI is the subject of a Breach, Security Incident, or use or disclosure of PHI not provided for by this Agreement that includes the information noted in Section III.F.4 – III.F.11 above.

G. Business Associate must, and is expected to, directly and independently fulfill all notification requirements under HIPAA.

H. In the event of a Breach, Security Incident, or use or disclosure of PHI not provided for by this Agreement, Business Associate must mitigate, to the extent practicable, any harmful effects of said disclosure that are known to it.

I. In accordance with 45 CFR §§ 164.502(e)(1)(ii) and 164.308(b)(2), Business Associate agrees to ensure that any agent, subcontractor, or employee to whom it provides PHI (received from, or created or received by, Business Associate on behalf of Covered Entity) agrees to the same restrictions, conditions, and requirements that apply through this Agreement to Business Associate with respect to such information.

J. Business Associate must ensure that any contract or other arrangement with a subcontractor meets the requirements of paragraphs 45 CFR §164.314(a)(2)(i) and (a)(2)(ii) required by 45 CFR § 164.308(b)(3) between a Business Associate and a subcontractor, in the same manner as such requirements apply to contracts or other arrangements between a Covered Entity and Business Associate.

K. Pursuant to 45 CFR § 164.502(a)(4)(ii), Business Associate must disclose PHI to the Covered Entity, Individual, or Individual's designee, as necessary to satisfy a Covered

ATTACHMENT C

Entity's obligations under § 164.524(c)(2)(ii) and (3)(ii) with respect to an individual's request for an electronic copy of PHI.

L. To the extent applicable, Business Associate must provide access to PHI in a Designated Record Set at reasonable times, at the request of Covered Entity or as directed by Covered Entity, to an Individual specified by Covered Entity in order to meet the requirements under 45 CFR § 164.524.

M. A Business Associate that is a health plan, excluding an issuer of a long-term care policy falling within paragraph (1)(viii) of the definition of health plan, must not use or disclose PHI that is genetic information for underwriting purposes, in accordance with the provisions of 45 CFR 164.502.

N. To the extent applicable, Business Associate must make any amendment(s) to PHI in a Designated Record Set that Covered Entity directs or agrees to, pursuant to 45 CFR § 164.526, at the request of Covered Entity or an Individual.

O. Business Associate must, upon request with reasonable notice, provide Covered Entity access to its premises for a review and demonstration of its internal practices and procedures for safeguarding PHI.

P. Business Associate must, upon request and with reasonable notice, furnish to Covered Entity security and privacy audit results, risk analyses, security and privacy policies and procedures, details of previous Breaches and Security Incidents, and documentation of controls.

Q. Business Associate must also maintain records indicating who has accessed PHI about an Individual in an electronic designated record set and information related to such access, in accordance with 45 C.F.R. § 164.528. Business Associate must document such disclosures of PHI and information related to such disclosures as would be required for a Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. § 164.528. Should an Individual make a request to Covered Entity for an accounting of disclosures of his or her PHI pursuant to 45 C.F.R. § 164.528, Business Associate must promptly provide Covered Entity with information in a format and manner sufficient to respond to the Individual's request.

R. Business Associate must, upon request and with reasonable notice, provide Covered Entity with an accounting of uses and disclosures of PHI that was provided to it by Covered Entity.

S. Business Associate must make its internal practices, books, records, and any other material requested by the Secretary relating to the use, disclosure, and safeguarding of PHI received from Covered Entity available to the Secretary for the purpose of determining compliance with HIPAA. Business Associate must make the aforementioned information available to the Secretary in the manner and place as designated by the Secretary or the Secretary's duly appointed delegate. Under this Agreement, Business Associate must comply and cooperate with any request for documents or other information from the Secretary directed to

ATTACHMENT C

Covered Entity that seeks documents or other information held or controlled by Business Associate.

T. Business Associate may use PHI to report violations of law to appropriate Federal and State authorities, consistent with 42 C.F.R. § 164.502(j)(1).

U. Except as otherwise limited in this Agreement, Business Associate may disclose PHI for the proper management and administration of Business Associate or the Underlying Agreement, provided that disclosures are Required By Law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and be used or further disclosed only as Required By Law or for the limited purpose for which it was disclosed to the person, and the person must agree to notify Business Associate of any instance of any Breach, Security Incident, or use or disclosure of PHI not provided for by this Agreement of which it is aware in which the confidentiality of the information has been breached.

V. Business Associate understands that, pursuant to 45 CFR § 160.402, the Business Associate is liable, in accordance with the Federal common law of agency, for a civil money penalty for a violation of the HIPAA rules based on the act or omission of any agent of the Business Associate, including a workforce member or subcontractor, acting within the scope of the agency.

IV. TERM AND TERMINATION.

A. Term. The Term of this Agreement shall be effective as of the effective date of the Underlying Agreement, and shall terminate: (1) when all of the PHI provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity; or, (2) if it is infeasible to return or destroy PHI, in accordance with the termination provisions in this Article IV.

B. Termination for Cause. Upon Covered Entity's knowledge of a material breach of this Agreement by Business Associate, Covered Entity shall:

1. Provide an opportunity for Business Associate to cure the breach or end the violation and, if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity, have the right to terminate this Agreement and to terminate the Underlying Agreement, and shall report the violation to the Secretary;

2. Have the right to immediately terminate this Agreement and the Underlying Agreement if Business Associate has breached a material term of this Agreement and cure is not possible, and shall report the violation to the Secretary; or

3. If neither termination nor cure is feasible, report the violation to the Secretary.

ATTACHMENT C

4. This Article IV, Term and Termination, Paragraph B, is in addition to the provisions set forth in Paragraph 27, Termination for Default of the General Conditions of Contract Between County and Contractor, attached to the Underlying Agreement, in which "Business Associate" is "Contractor" and "Covered Entity" is "County" for purposes of this Agreement.

C. Effect of Termination.

1. Except as provided in Section IV.C.2, upon termination or cancellation of this Agreement, for any reason, Business Associate must return or destroy all PHI received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision applies to PHI that is in the possession of a subcontractor(s), employee(s), or agent(s) of Business Associate. Business Associate must not retain any copies of the PHI.

2. In the event that Business Associate determines that returning or destroying the PHI is infeasible, Business Associate must provide to Covered Entity written notification of the nature of the PHI and the conditions that make return or destruction infeasible. After written notification that return or destruction of PHI is infeasible, Business Associate must extend the protections of this Agreement to such PHI and limit further use(s) and disclosure(s) of such PHI to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such PHI. Notwithstanding the foregoing, to the extent that it is not feasible to return or destroy such PHI, the terms and provisions of this Agreement survive termination of this Agreement with regard to such PHI.

3. Should Business Associate violate this Agreement, HIPAA, the Underlying Agreement, the MCMRA, or other applicable law, Covered Entity has the right to immediately terminate any contract then in force between the Parties, including the Underlying Agreement.

V. CONSIDERATION. Business Associate recognizes that the promises it has made in this Agreement shall, henceforth, be reasonably, justifiably, and detrimentally relied upon by Covered Entity in choosing to continue or commence a business relationship with Business Associate.

VI. CAUSES OF ACTION IN THE EVENT OF BREACH. As used in this paragraph, the term "breach" has the meaning normally ascribed to that term under the Maryland law related to contracts, as opposed to the specific definition under HIPAA related to PHI. Business Associate hereby recognizes that irreparable harm will result to Covered Entity in the event of breach by Business Associate of any of the covenants and assurances contained in this Agreement. As such, in the event of breach of any of the covenants and assurances contained in this Agreement, Covered Entity shall be entitled to enjoin and restrain Business Associate from any continued violation of this Agreement. Furthermore, in the event of breach of this Agreement by Business Associate, Covered Entity is entitled to reimbursement and indemnification from Business Associate for Covered Entity's reasonable attorneys' fees and expenses and costs that were reasonably incurred as a proximate result of Business Associate's breach. The causes of action

ATTACHMENT C

contained in this Article VI are in addition to (and do not supersede) any action for damages and/or any other cause of action Covered Entity may have for breach of any part of this Agreement. Furthermore, these provisions are in addition to the provisions set forth in Paragraph 18, "Indemnification", of the General Conditions of Contract Between County and Contractor, attached to the Underlying Agreement in which "Business Associate" is "Contractor" and "Covered Entity" is "County", for purposes of this Agreement.

VII. MODIFICATION; AMENDMENT. This Agreement may be modified or amended only through a writing signed by the Parties and, thus, no oral modification or amendment hereof shall be permitted. The Parties agree to take such action as is necessary to amend this Agreement, from time to time, as is necessary for Covered Entity to comply with the requirements of HIPAA, including its Privacy, Security, and Notice Rules.

VIII. INTERPRETATION OF THIS AGREEMENT IN RELATION TO OTHER AGREEMENTS BETWEEN THE PARTIES. Should there be any conflict between the language of this Agreement and any other contract entered into between the Parties (either previous or subsequent to the date of this Agreement), the language and provisions of this Agreement, along with the Underlying Agreement, shall control and prevail unless the Parties specifically refer in a subsequent written agreement to this Agreement, by its title, date, and substance and specifically state that the provisions of the later written agreement shall control over this Agreement and Underlying Agreement. In any event, any agreement between the Parties, including this Agreement and Underlying Agreement, must be in full compliance with HIPAA, and any provision in an agreement that fails to comply with HIPAA will be deemed separable from the document, unenforceable, and of no effect.

IX. COMPLIANCE WITH STATE LAW. The Business Associate acknowledges that by accepting the PHI from Covered Entity, it becomes a holder of medical records information under the MCMRA and is subject to the provisions of that law. If HIPAA conflicts with another applicable law regarding the degree of protection provided for Protected Health Information, Business Associate must comply with the more restrictive protection requirement.

X. MISCELLANEOUS.

A. Ambiguity. Any ambiguity in this Agreement shall be resolved to permit Covered Entity to comply with HIPAA.

B. Regulatory References. A reference in this Agreement to a section in HIPAA means the section in effect, or as amended.

C. Notice to Covered Entity. Any notice required under this Agreement to be given Covered Entity shall be made in writing to:

Joy Page, Esq.
Deputy Privacy Official
Montgomery County, Maryland
401 Hungerford Drive, 7th Floor
Rockville, Maryland 20850

ATTACHMENT C

(240) 777-3247 (Voice)
(240) 777- 3099 (Fax)

Notice to Business Associate. Any notice required under this Agreement to be given Business Associate shall be made in writing to:

Address: 103 Old Court Rd. Suite A
Baltimore, MD
Attention: Raffi Bilek
Phone: 443-598-2821

D. Maryland Law. This Agreement is governed by, and shall be construed in accordance with, applicable federal law and the laws of the State of Maryland, without regard to choice of law principles.

E. Incorporation of Future Amendments. Other requirements applicable to Business Associates under HIPAA are incorporated by reference into this Agreement.


F. Penalties for HIPAA Violation. In addition to that stated in this Agreement, Business Associate may be subject to civil and criminal penalties noted under HIPAA, including the same HIPAA civil and criminal penalties applicable to a Covered Entity.

SIGNATURE PAGE FOLLOWS

ATTACHMENT C

IN WITNESS WHEREOF and acknowledging acceptance and agreement of the foregoing, the Parties affix their signatures hereto.

THE BALTIMORE THERAPY CENTER,
LLC

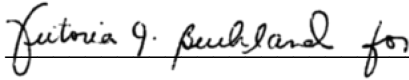
By: 

Name: Raffi Bilek

Title: Director

Date: 8/25/2020

MONTGOMERY COUNTY, MARYLAND

By: 

Name: Raymond L. Crowel, Psy. D.

Title: Director, Department of Health &
Human Services

Date: 8/14/2020

ATTACHMENT C

EXHIBIT A

FORM OF NOTIFICATION

This notification is made pursuant to Section III.F of the Business Associate Agreement between:

- Montgomery County, Maryland, (the “County”) and
- The Baltimore Therapy Center, LLC (Business Associate).

Business Associate hereby notifies the County that there has been a Breach, Security Incident, or use or disclosure of PHI not provided for by the Business Associate Agreement (an “Incident”) that Business Associate has used or has had access to under the terms of the Business Associate Agreement.

Description of the Incident:

Date of the Incident: _____

Date of discovery of the Incident: _____

Does the Incident involve 500 or more individuals? Yes/No

If yes, do the people live in multiple states? Yes/No

Number of individuals affected by the Incident:

Names and addresses of individuals affected by the Incident:

(Attach additional pages as necessary) _____

The types of unsecured PHI that were involved in the Incident (such as full name, Social Security number, date of birth, home address, account number, or disability code):

Description of what Business Associate is doing to investigate the Incident, to mitigate losses, and to protect against any further Incidents:

ATTACHMENT C

Contact information to ask questions or learn additional information:

Name: _____

Title: _____

Address: _____

Email Address: _____

Phone Number: _____



Marc Elrich
County Executive

OFFICE OF THE 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

A handwritten signature in black ink, likely of the County Executive, over the CAO APPROVAL text.

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.



MONTGOMERY COUNTY ADMINISTRATIVE PROCEDURE

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

NO.
6-7

PAGE
2 OF 5

DATE
12/20/2019

CAO APPROVAL

A handwritten signature in black ink, appearing to be "JH", written over the "CAO APPROVAL" text.

Information Security

- 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.



MONTGOMERY COUNTY ADMINISTRATIVE PROCEDURE

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

NO.
6-7

PAGE
3 OF 5

DATE
12/20/2019

CAO APPROVAL

Information Security

- 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.



MONTGOMERY COUNTY ADMINISTRATIVE PROCEDURE

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

NO.
6-7

PAGE
4 OF 5

DATE
12/20/2019

CAO APPROVAL

Information Security

- 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.



MONTGOMERY COUNTY ADMINISTRATIVE PROCEDURE

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

NO.
6-7

PAGE
5 OF 5

DATE
12/20/2019

CAO APPROVAL

A handwritten signature in black ink, appearing to be "FR", written over the "CAO APPROVAL" text.

Information Security

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 Backup 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.

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, Department 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 rationale 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.




OFFICE OF THE COUNTY EXECUTIVE
ROCKVILLE, MARYLAND 20850

Isiah Leggett
County Executive

MEMORANDUM

September 2, 2010

To: Department/Office Directors; and
ASCs and Functional Equivalents

FROM:  Fariba Kassiri, Assistant Chief Administrative Officer

SUBJECT: Administrative Procedure 6-1, Use of County-Provided Internet, Intranet, and Electronic Mail Services

Please go to OMB's website to find Administrative Procedure 6-1, Use of County-Provided Internet, Intranet, and Electronic Mail Services under the Information and Processing Section of the Administrative Procedure Manual. The Administrative Procedure provides employees with guidelines governing the use of County-provided Internet, intranet, and electronic mail services by County employees. The County maintains intranet and internet access for its employees for the purpose of improving productivity, professional development, and the level of service to the people of our community.

A County employee may use County-provided Internet, intranet, or email services for personal purposes on only a limited, reasonable basis, and in accordance with this administrative procedure. However, employees must act reasonably to minimize personal use of County-provided Internet, intranet, and email services. Personal use of County Internet, intranet, or email services by employees 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 official duties.

The AP is being published in final form under the Information Processing Section on the AP website. Please forward this administrative procedure to all your division chiefs, program managers, and all other employees in supervisory capacity.

View the table of contents on OMB's home page on the intranet at
<http://portal.mcgov.org/Omb/forms/APs/AP.htm>

FK:pw



MONTGOMERY COUNTY ADMINISTRATIVE PROCEDURE

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

NO.
6-1

PAGE 1 OF 8

DATE
9/2/10

TITLE

Use of County-Provided Internet, Intranet, and E-mail Services

CAO APPROVAL

A handwritten signature in black ink, appearing to be "JW", written over the "CAO APPROVAL" text.

PURPOSE

- 1.0 To establish an administrative procedure governing the use of County-provided Internet, intranet, and electronic mail services by County employees. The County maintains intranet and Internet access for its employees for the purpose of improving productivity, professional development, and the level of service to the people of our community.

DEFINITIONS

- 2.0 Department of Technology Services (DTS) - A department in the executive branch that is responsible for automated information systems and telecommunications technology.
- 2.1 CIO - Chief Information Officer and DTS Department Head
- 2.2 Personal Use - Activity that is conducted for purposes other than accomplishing official or otherwise authorized activity.

POLICY

- 3.0 Internet, intranet, and electronic mail (email) services are provided to County employees and persons legitimately affiliated with the business of the County government for the efficient exchange of information and the completion of assigned responsibilities that are consistent with the County's purposes.
- 3.1 Employees must use County-provided Internet, intranet, and email services responsibly and professionally, and must not use Internet, intranet, or email services 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.
- 3.2 A County employee may use County-provided Internet, intranet, or email services for personal purposes on only a limited, reasonable basis, and in accordance with this administrative procedure. However, employees must act reasonably to minimize personal use of County-provided Internet, intranet, and email services. Personal use of County Internet, intranet or email services by employees 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 official duties.
- 3.3 An employee's use of County-provided Internet, intranet, or email services indicates 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 work-related misfeasance), of his/her electronically stored email messages and computer files, and any other data related to the employee's use of the County's Internet, intranet, and email services.



MONTGOMERY COUNTY ADMINISTRATIVE PROCEDURE

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

NO.
6-1

PAGE 2 OF 8

DATE
9/2/10

TITLE

Use of County-Provided Internet, Intranet, and E-mail Services

CAO APPROVAL

FK

- 3.4 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 laws and Regulations, and Ethics Laws, currently codified at Chapter 33, Appendix F, and Chapter 19A of the County Code, respectively, and applicable collective bargaining agreements, as amended.

GENERAL

CONNECTING TO INTERNET, INTRANET, AND EMAIL SERVICES

- 4.0 County employees may connect to County-provided Internet, intranet, or email services only through:
- A. Personal Computers (PCs) such as desktops and laptops connected to the County's computer network via the County's secure enterprise Internet service connection; or
 - B. Stand-alone (non network-connected or temporarily disconnected) PCs via a private Internet Service Provider (ISP), such as America On-Line (AOL), or via a DTS-sanctioned remote access method.
- 4.1 Any PC that connects to County-provided Internet, intranet, or email services must have up-to-date antivirus software and current updates for Windows operating system software installed on it and must be configured to actively protect against virus infections and periodically scan the PC to check for viruses.
- 4.2 Costs incurred by the County for ISP connections to stand-alone PCs are the responsibility of the using department. Employees must obtain department approval prior to obtaining a County-provided ISP connection.

PROHIBITED USER CONDUCT

- 4.3 Employees must use County-provided Internet, intranet, and email services in accordance with this administrative procedure and all applicable laws, regulations, and policies. Prohibited conduct, including personal use, includes:
- A. Accessing, sending, forwarding, storing, or saving on County PCs or servers 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.



MONTGOMERY COUNTY ADMINISTRATIVE PROCEDURE

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

NO.
6-1

PAGE 3 OF 8

DATE 9/2/10

TITLE

Use of County-Provided Internet, Intranet, and E-mail Services

CAO APPROVAL

FR

- B. Personal use beyond that permitted by this policy.
- C. Any use prohibited by federal, State, or County law.
- D. Employees may not modify computer equipment for personal purposes. This would include loading of personal software, non-County supplied software; "shareware" and/or "freeware"; 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.
- E. Using the County's Internet, intranet, or email services to gain unauthorized access to County or other system resources.
- F. Using the County's Internet, intranet, or email services for gambling or other illegal or County-prohibited activities.
- G. Using the County's Internet, intranet, or email services for private gain or profit.
- H. Infringing upon computer software and data protected by copyright intellectual property rights and/or license laws.
- I. Using the County Internet, intranet, or email services or applications to publish and/or represent (expressly or implicitly) personal or unofficial opinions as those of the County.
- J. Any personal use that could cause congestion, delay or disruption of service to any County system or equipment. This may include, but not limited to:
 - 1. "Chain" or unnecessary "Reply All" emails; and
 - 2. Downloads of video, sound or other large, non-work related files.
- K. Sending broadcast messages to all, or the majority of, County e-mail users without obtaining prior approval from the Chief Administrative Officer (CAO), in accordance with County information technology policies and procedures.

COUNTY OWNERSHIP, MONITORING, CONTROL, AND DISCLOSURE

- 4.4 All County-provided electronic systems, hardware, software, temporary or permanent files and any related systems or devices used in the transmission, receipt or storage of Internet, intranet, or email communications are the property of, or licensed to, the County.



MONTGOMERY COUNTY ADMINISTRATIVE PROCEDURE

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

NO.
6-1

PAGE 4 OF 8

DATE 9/2/10

TITLE

Use of County-Provided Internet, Intranet, and E-mail Services

CAO APPROVAL

FK

- 4.5 Any information transmitted or received by employees using the County's Internet, intranet, and email services, or stored on the County's computer resources, is the property of the County and, therefore, is not considered private. This includes email from an employee's personal account, such as Hotmail or AOL, if that email is stored on the County's computer resources.
- 4.6 Internet, intranet, and email electronic files and messages may be retrieved from storage by the County and its agents without prior notice to an employee, even if the electronic files and messages have been deleted by the sender or receiver. These messages and files may also be used by the County in disciplinary or other proceedings.
- 4.7 Employees must take appropriate measures to prevent unauthorized access to confidential information when using the County's Internet, intranet, and email services, in accordance with applicable federal, State, or Montgomery County laws, regulations, or policies regarding confidential information.
- 4.8 The County may monitor an employee's use of County-provided Internet, intranet, and email services, and may access an employee's email messages and computer files in its sole discretion, 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, such as Hotmail or AOL, if the personal email is stored on the County's computer resources.
- 4.9 Upon the approval of the email user's department head and the CIO, system administrators in DTS or the email user's department may access an employee's email messages and computer files related to the employee's use of the County's Internet, intranet, and email services. The existence of privately held passwords and "message delete" functions do not restrict or eliminate the County's ability or right to access this information.
- 4.10 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.
- 4.11 The County may be compelled to access and disclose to third parties messages sent over its Internet, intranet, or email systems, in accordance with the Maryland Public Information Act (MPIA), Maryland Code Ann., State Gov't §§ 10-611 to 10-628 (1998 Repl. Vol.). 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).



MONTGOMERY COUNTY ADMINISTRATIVE PROCEDURE

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

NO.
6-1

PAGE 5 OF 8

DATE 9/2/10

TITLE

Use of County-Provided Internet, Intranet, and E-mail Services

CAO APPROVAL

FK

RESPONSIBILITIES

5.0 Department of Technology Services

- A. Provide a 24-hour, 7 day-a-week secure, high-speed enterprise connection to Internet, intranet, and email services.
- B. Notify users of County-provided Internet, intranet, and email services when those services will be unavailable for system or network maintenance.
- C. Provide operating system and anti-virus software for all County-owned PCs, and manage software configurations, including operating system and anti-virus, for all County-owned PCs connected to the County's network.
- D. Accept help desk calls when a County employee or department notes a problem with County-provided Internet, intranet, or email services, and distribute information, updates, and/or resolutions, as appropriate.
- E. Maintain the current version of this administrative procedure, in accordance with Administrative Procedure 6-6, Information Technology Policies and Procedures Manual.
- F. Provide CIO approval or denial of a department head's request to monitor an employee's use of County-provided Internet, intranet, and email services, or to access an employee's email messages and computer files.
- G. Provide information to a department head regarding an employee's use of County-provided Internet, intranet, and email services, when directed by the CIO to do so.

5.1 Department

- A. Ensure that employees are informed of, and comply with, this administrative procedure.
- B. Responsible to ensure the appropriate use of department resources, including IT and official employee time.
- C. Ensure that this administrative procedure is incorporated by reference into all contracts in which the County is to provide contractors or volunteers with the use of its Internet, intranet, or email services to conduct the County's business, and that all contractors and volunteers are bound to comply with this administrative procedure.



MONTGOMERY COUNTY ADMINISTRATIVE PROCEDURE

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

NO.
6-1

PAGE 6 OF 8

DATE 9/2/10

TITLE

Use of County-Provided Internet, Intranet, and E-mail Services

CAO APPROVAL

PK

- D. Pay the cost of ISP services or remote access connections that it approves for non-networked PCs.
- E. Manage the configuration of anti-virus software for non-networked, County-owned PCs, and obtain from DTS any necessary anti-virus software.
- F. Through DTS or departmental IT staff, ensure that the operating system on PCs have software updates in accordance with County information technology policies and procedures.
- G. A Department head must seek approval from the CIO prior to monitoring or accessing an employee's electronically-stored email messages or computer files, or any other electronically-stored information available related to the employee's use of the County's Internet, intranet, and email services.

5.2 County Employees

- A. Keep apprised of the latest version of this administrative procedure.
- B. Ensure use of County-provided Internet, intranet, and email services is in accordance with this administrative procedure.
- C. Must not access another user's email account without authorization from the department director or the employee to whom the email account is assigned.
- D. Obtain department approval prior to acquiring a County-provided ISP connection for a non-networked PC.
- E. In accordance with County information technology policies and procedures, obtain approval from the CAO before sending a broadcast email to all, or the majority of, County email users.

PROCEDURE

- 6.0 Employee Abide by this administrative procedure as it relates to the use of Internet, intranet, and email services.
- 6.1 Department Ensure that all employees are informed of and abide by this administrative procedure.

ISP Connection on Non-Networked Computer

- 6.2 Employee Request approval from department for the acquisition of a County-provided ISP connection for a non-networked PC.



MONTGOMERY COUNTY ADMINISTRATIVE PROCEDURE

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

NO.
6-1

PAGE 7 OF 8

DATE 9/2/10

TITLE

Use of County-Provided Internet, Intranet, and E-mail Services

CAO APPROVAL

FIL

6.3 Department

Approve or disapprove of the employee's request for a County-provided ISP connection for a non-networked PC.

Pay the costs of any approved ISP services that result from the employee's request.

Broadcast email

6.4 Employee

Request approval from department for sending a broadcast email to all, or the majority of County employees.

6.5 Department

Request approval from the CAO prior to permitting an employee to send a broadcast email to all, or the majority of, County employees.

6.6 CAO

Approve or disapprove requests to send County-wide broadcast email messages.

Monitoring and Accessing Use

6.7 Department

Determine if there is a legitimate business purpose to monitor an employee's use of County-provided Internet, intranet, and email services, or to access an employee's email messages or computer files.

If there is a legitimate business purpose to monitor an employee's use of County-provided Internet, intranet, and email services, the department head must request in writing to the CIO for approval to monitor an employee's use of County-provided Internet, intranet, and email services or to access an employee's email messages or computer files.

6.8 CIO

Approve or disapprove a department head's request for monitoring or accessing an employee's email messages or computer files.

6.9 DTS

For approved requests, provide appropriate information to the requesting department head.



MONTGOMERY COUNTY ADMINISTRATIVE PROCEDURE

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

NO.
6-1

PAGE 8 OF 8

DATE 9/2/10

TITLE

Use of County-Provided Internet, Intranet, and E-mail Services

CAO APPROVAL

FK

DEPARTMENTS AFFECTED

7.0 All County Departments.