Maine
Cumberland County

Administrative Regulations & Policies

AMENDMENTS EFFECTIVE: September 11, 2023

Cumberland County Government
142 Federal Street, Portland, ME 04101

Table of Contents

APPENDICES

AMENDMENTS TO ADMINISTRATIVE REGULATIONS

1.	*November 2019*		
2.	*March 2020*		
3.	*September 2020*		
4.	*July 2021*		
5.	*November 2021*		
6.	*June 2022*		
7.	*December 2022*		
8.	*September 2023*		

#1: Administrative Regulations

I. SCOPE

All employees of the County of Cumberland will be guided in administrative policy by the Administrative Code as set forth in the County Charter, Section 4.2.3. These administrative regulations will be issued or amended from time to time by the County Manager and submitted to the Commissioners for adoption.

II. SUBJECT MATTER

The Administrative Code will include regulations concerning Programs, Procedures and Policies that are important to the operation of the County.

III. MAINTENANCE OF REGULATIONS

The Executive Office and Human Resources Office are responsible for maintaining and updating the Administrative Regulations on the County's Intranet to meet the needs of the organization. Employees shall be informed of new or revised regulations by the HR Office.

IV. PREPARATION OF ADMINISTRATIVE REGULATIONS

When Department Heads or other County officials become aware of situations requiring clarification as to specific policy, they should prepare a proposed Administrative Regulation for the County Manager's consideration.

V. ISSUANCE OF ADMINISTRATIVE REGULATIONS

Administrative Regulations may only be issued by the County Manager, or in cases of prolonged absence or disability of the County Manager, they may be issued by an Acting County Manager or Director of Finance and Administration if warranted by circumstances with final review and adoption by the Board.

EFFECTIVE: March 11, 2019

#2: Employee Recognition Awards

I. ACTS OF COURTESY AND EXCELLENCE AWARD (ACE)

A. Purpose

The A*C*E Award is designed to recognize employees who exhibit a positive attitude, reflected in their outstanding service, to both internal and external customers. The goal is to furnish employees with a means by which they may be recognized for their assistance and cooperation, foster employee drive for excellence, including increased productivity and boost employee morale.

B. Criteria for Evaluation of Nominees

Activities to be considered for A*C*E* Awards include:

- performance which substantially exceeds the expected level of performance over a sustained period of time;
- performance on a specific project or assignment that exceeds all normal expectations;
- performance of assigned duties with special effort or special innovation that results in significant cost savings or other highly desirable benefits to operations;
- exemplary or courageous handling of an emergency situation related to official employment; and
- a special act or service in the public interest which clearly warrants special recognition.

C. Eligibility

All employees who are non-management, full and part time, are eligible for an A*C*E* Award. Nominees must have at least one year of service, no written discipline in the past year, and/or no suspensions in the past three (3) year period. Nominees must not have received the award in the previous year.

1. Management is defined as Paygrade 11 and above, as listed in the County Personnel Employee Position Classification Plan. Nominees at Paygrade 11 and above will not be considered.

D. Nominations

Any employee, citizen or County business owner, except an immediate family member, is eligible to submit a nomination form to the Human Resources Office for an A*C*E* Award. The employee's Supervisor and Department Head will review the nomination and may provide comments to the Employee Advisory Committee (EAC), charged by the County Manager with the responsibility of providing final evaluation of candidates for the award. A courtesy copy of the nomination will be provided to the nominee's department head, supervisor, and employee and will be placed in the employee's personnel file.

Nominations must be received by the EAC by December 31 to be considered. Nominations received after December 31 will be considered for the following calendar year.

E. Type of Award

A monetary award in the amount of $150.00 net will be presented, along with a certificate of appreciation.

II. SERVICE AWARD

A. Purpose

The Service Award provides recognition for an employee's length of dedicated service to the County of Cumberland.

B. Eligibility

All regular full and part time employees are eligible for awards that commence with five years of continuous service.

C. Awards and Criteria

Employees eligible for an award during the calendar year will be recognized for 5 year increments of service (5, 10, 15, 20, etc.) at the annual awards ceremony.

D. Years of Service is determined by the Employee's Hire Date in MUNIS.

E. Years of Service is defined by uninterrupted employment.

III. CUMBERLAND COUNTY EMPLOYEE OF THE YEAR

A. Purpose

The Cumberland County Employee of the Year is the most prestigious award and provides recognition for outstanding achievement in public service.

B. Eligibility

The Employee of the Year will be voted on from the eligible nominations received for the A*C*E Award.

C. Award

A monetary award in the amount of $500.00 net will be presented, along with a certificate of appreciation.

IV. ATTACHMENTS

***APPENDIX A1**: A*C*E (Acts of Commitment and Excellence) Nomination Form*

EFFECTIVE: March 11, 2019

#3: FOAA Schedule of Fees

I. SCOPE

The Maine Freedom of Access Act ("FOAA") grants the people of this state a broad right of access to public records while protecting legitimate governmental interests and the privacy rights of individual citizens. FOAA requests shall be handled per Maine State Statute.

The County's Public Information Officer shall keep track of those FOAA requests that departments receive with the exception of Regional Communications, District Attorney and Sheriff's Office/Jail.

The Public Information Officer in each of the above locations will be the contact with requester and be the point person for the collection of data and material for the request. The fee schedule should be reviewed and, if needed, updated annually.

II. COSTS ASSOCIATED WITH REQUEST:

A. Employee Time

First 2 hours free and Additional Hours charged at $25.00 per hour, if greater than $30, the requester must be notified before proceeding with the request. If greater than $100, may require a requester to pay all or a portion of the estimated costs to complete the request

B. Photocopies

10 cents each (If an agency doesn't have the technical ability to redact electronically then they are not under an obligation to provide records in electronic medium. 1 M.R.S. section 408-A(7))

C. Color photocopies

$2.00/each

D. Non-paper copies requests

$25.00

E. Dispatch Transcripts

$25.00

III. SHERIFF'S OFFICE

The Sheriff's Office manages their own fee schedule for FOAA requests. View **Appendix B1** for rates.

IV. ATTACHMENTS

***Appendix B1**: Schedule of Fees CCSO*

AMENDMENT EFFECTIVE: NOVEMBER 8, 2021

#4: Meal Allowance

I. PURPOSE

The purpose of this policy is to establish meal reimbursement rates for County employees.

II. POLICY

Employees required to travel and/or use personal conveyances on official business for the County will be reimbursed for such expenses as food, lodging and transportation as may be incurred while on such official business of the County.

Meal expenses are divided between the following categories: Same Day, and Multi-Day. Same day meal expenses are those that have been approved for one-day events, typically but not necessarily within the state of Maine. Multi-Day expenses are those that require an employee to spend multiple days outside of their normal work environment and seek outside lodging, and may be located within the state of Maine.

The limits for expenses are as follows:

A. Same Day Meal Reimbursements

Same day meal expenses will have the following maximum allowances including all taxes and tips:

1. Breakfast: $12
2. Lunch: $15
3. Dinner: $25

B. Multi-Day Meal Reimbursements

Multi-day meal expenses will have the following maximum allowances including all taxes and tips:

1. Breakfast: $15
2. Lunch: $20
3. Dinner: $30

C. Personal Conveyance

Reimbursement for personal conveyance will be set at such rate as may be set forth by County Administrative Regulations.

EFFECTIVE: March 11, 2019

#5: Purchasing Policy

I. PURPOSE

The purpose of this policy is to promulgate the various purchasing procedures to be utilized by all County departments as well as Committees that are part of the budget appropriations.

It is the responsibility of the County to make purchases of goods or services required in a manner that best secures the greatest possible economy consistent with the required grade or quality of the goods or services. Except as otherwise provided by state statutes, the County shall make the purchase of goods and services as stated in this policy.

II. ROUTINE AND SMALLER PURCHASES

A. Purchases that are routine and ongoing in nature do not require Purchase Orders. These are items that would ordinarily be purchased many times during the course of a year. Purchases made once per year, such as replacement vehicles, are not considered routine in nature. Examples of such purchases would include, but are not limited to:

1. On-going utility charges including heating fuel purchases
2. Electricity
3. Telephone and Cell Phone bills
4. Regular payments for previously approved contracted services
5. Maintenance and repair contracts
6. Copier bills
7. Postage
8. Travel and meeting reimbursements
9. Restitution payments
10. Equipment rental
11. Advertising
12. Dues and Subscription
13. Regularly occurring food purchases (CCJ)
14. Routine cleaning supplies
15. Emergency repairs and maintenance

B. Purchases under $100 do not require a Purchase Order. Only an approved and properly coded invoice is required for payment. Splitting up purchases to stay under this limit is not allowed. For example, placing four $99 orders for four single new tires for a vehicle is considered an intentionally misleading act, and can warrant disciplinary action.

C. Any questions as to whether or not a purchase order is required should be directed to the county Finance Director. It is understood that there will invariably be purchases where no clear-cut rules exist, and in these instances, the Finance Director will do their best to find a logical and simple solution.

III. ANNUAL TIME AND MATERIALS BID

The County Manager and/or Finance Director shall have the authority to contract for professional, trades and other services or materials through a time and material bid, provided that all such contracts in excess of seventy-five thousand dollars ($75,000) shall be approved by the County Commissioners.

IV. PURCHASES REQUIRING A PURCHASE ORDER

A. Purchases not excluded as outlined in item A.1. that exceed $100 require an approved Purchase Order before a purchase can be made.

B. Applicable purchases between $100 and $999 require the approval of the appropriate Department Head before a purchase can be made.

C. Applicable purchases between $1000 and $4999 require the approval of both the appropriate Department Head and the Finance Director before a purchase can be made.

V. USE OF REQUISITION AND PAYMENT REQUEST FORMS

Departments that choose to use their own payment request or requisition forms are free to continue to do so if they feel it best suits their needs. Because the size and functions of the individual departments vary widely within the county, there will never be "one-size-fits-all" solution for all departments. For example, the approval chain of a small department like HR does not need to be nearly as extensive as the jail. For that reason, departments are free add their own approval methods as they see fit as long as it does not interfere with the existing PO process.

VI. PURCHASES REQUIRING COUNTY MANAGER APPROVAL

Any purchase that would ordinarily require a Purchase Order and Finance Director approval and has not been specifically budgeted requires the prior approval of the County Manager before a purchase can be made. Examples would include unbudgeted vehicle purchases, remodeling of a work area, or adding a large photocopier to an area that has no budget for such an item. Any questions as to whether or not County Manager approval is needed should be directed to either the County Manager and/or Finance Director.

VII. BIDS, AWARDS, AND CONTRACTS

A. Purchases for goods or services which involve expenditures of less than $15,000 can be made after price shopping has been conducted for the best all-around cost and quality for the product desired.

B. Purchases for goods or services which involve expenditures of $15,000 to $75,000, wherever possible, be based on at least three (3) quotes, and shall be awarded to the most responsive and responsible bidder.

C. The County may accept contract pricing for goods or services, however it is not obligated to purchase from the guaranteed rate vendor if a lower price is available.

D. The procurement of goods or services which involves expenditures of more than $75,000 must be done through a competitive advertised bid process and shall be awarded to the most responsive and responsible bidder.

VIII. COMPETITIVE BID PROCESS

A. The County Manager shall ensure that the requesting department prepares the invitation to bid to include:

1. specifications required;
2. have notice informing the public;
3. receive sealed bids;
4. hold a public bid opening.

B. The bid shall be awarded to the lowest most responsive and responsible bidder that meets the specifications and submits proper bond requirements if applicable. The Board of Commissioners shall make the final decision if supporting information justifies other than the low bid be awarded.

IX. EXEMPTION FROM COMPETITIVE BIDDING

The competitive bid process may be waived by the Board of Commissioners or the County Manager on the following circumstances:

A. Exemption from bidding procedures--Emergency purchases.

1. *By head of departments.* In case of actual emergency, and with the approval of the county manager or finance director, the head of any using department may purchase directly any supplies, general services or improvements whose immediate procurement is essential to prevent delays in the work of the using department which may vitally affect the life, health or convenience of citizens or employees.

2. Recorded explanation. The head of such using department shall send to the County Manager or finance director a requisition and a copy of the delivery record together with a full written report of the circumstances of the emergency. The report shall be filed with the county manager or finance director, and where the amount of the purchase exceeds seventy-five thousand dollars ($75,000.00), to the commissioners.

B. Exemption from competitive bidding--Cooperative purchasing; used equipment auctions.

1. Staff shall have the authority to join with other units of government in cooperative purchasing plans when the best interests of the county would be served thereby. The requirements of formal and informal bidding shall not apply to such cooperative arrangements.

2. Staff, upon the approval of the County Manager or Finance Director, shall have the ability to use a recent town or county competitive bid for the same product being purchased. The competitive bid used shall not be more than eight months old.

3. The County Manager and/or the Finance Director may authorize on an item by item basis, to purchase used equipment at public auction without using either formal or informal bidding procedures where the County Manager and/or Finance Director has determined it would be in the County's best financial interest.

C. Exemption from competitive bidding--Sole source.

1. Occasions may arise when competition among vendors is not possible for a particular purchase (example: proprietary controls/software etc) and going out to bid could yield significant cost. The County Manager and the Finance Director may approve negotiated procurement of goods or services without requiring bids if it is determined from all information submitted by the department head to the county manager that steps were taken to verify that the necessary features provided by the proposed vendor are not available from other vendors; that the use of a specific product, manufacturer or vendor is required to maintain consistency of equipment; and that no similar standard goods would reasonably satisfy the county's requirements.

D. Exemption from bidding – Negotiated Purchase

1. Where there has been competitive bidding either formal or informal but no bids were received or the County Manager or Finance Director has rejected all bids because the bid prices were unreasonable or none of the bids met specifications, the department head or his/her designee may negotiate for purchases. A purchase by negotiation shall be approved by the County Manager or, if in excess of seventy-five thousand dollars ($75,000), by the County Commissioners.

X. PROPRIETY EQUIPMENT

All vendors bidding on equipment, services or fixed assets within county departments shall be an authorized dealer in the proprietary equipment being bid at the time of submitting an informal or formal bid. The vendor shall submit at time of bid proof of holding a proprietary license/certificate/vendor ID or equivalent showing their ability to participate in the bid.

XI. PAYMENT FOR GOODS OR SERVICES

A. Payment requests for any routine or smaller purchases as defined in section

1. Require approval from the Department, the account to be charged, and a valid invoice or payment request form.

B. Payment requests for any purchases requiring a Purchase Order will require

1. Purchase Order
2. Approval from the Department and/or Finance Director (on P.O.)
3. Account to be charged (on P.O.)
4. Original Invoice

C. Payment requests for any purchases requiring the competitive bid process will require:

1. Requisition
2. Request for Quotation Form
3. Purchase Order
4. Approval from the Department and/or Finance Director (on P.O.)

5. Account to be charged (on P.O.)
6. Original Invoice

XII. STAFF REPORTS FOR THE COMMISSIONERS

A. Commissioners are the only authority to bind the County in leases and long-term contractual agreements.

B. Staff reports will be provided for all contracts, and leases for presentation, approval and explanation at defined Commissioner's meetings.

C. Staff reports may be approved directly by the County Manager in these applications:

1. Copier Leases and other small office leases for equipment
2. Mileage Reimbursement Increases
3. And general housekeeping operating agreements on a case by case basis

AMENDMENTS TO THRESHOLDS - EFFECTIVE: NOVEMBER 8, 2021

#6: Payment Card Security Policy

I. INTRODUCTION

To safeguard Cumberland County's information technology resources and to protect the confidentiality of data it receives, holds or processes, the County, as well as users of that data and of the County's technology, resources must take adequate security measures. This Information Security Policy reflects Cumberland County's commitment to comply with reasonable and recognized standards governing the security of sensitive and confidential information.

Cumberland County can minimize inappropriate exposures of confidential and/or sensitive information, loss of data and inappropriate use of computer networks and systems by complying with reasonable and recognized standards (such as the Payment Card Industry Data Security Standard), attending to the proper design and control of information systems, and applying sanctions when violations of this security policy occur.

Security is the responsibility of everyone who uses Cumberland County's information technology resources. It is the responsibility of employees, contractors, business partners, and agents of Cumberland County. Each must become familiar with this policy's provisions and the importance of adhering to it when using Cumberland County's computers, networks, data and other information resources. Each is responsible for reporting any suspected breaches of the terms of this policy. As such, all information technology resource users are expected to adhere to all policies and procedures mandated by the County's Director of Information Technology.

II. PURPOSE/SCOPE

The primary purpose of this security policy is to establish rules to ensure the protection of confidential and/or sensitive information stored or transmitted electronically to or by Cumberland County, and to ensure protection of Cumberland County's information technology resources. The policy assigns responsibility and provides guidelines to protect the County's systems and data against misuse and/or loss.

This security policy applies to all users of computer systems, centrally managed computer systems, or computers that are part of or are authorized to connect to Cumberland County's data network.

It may apply to users of information services operated or administered by Cumberland County (depending on access to sensitive data, etc.). Individuals working for institutions affiliated with Cumberland County are subject to these same definitions and rules when they are using the County's information technology resources.

This security policy applies to all aspects of information technology resource security including, but not limited to, accidental or unauthorized destruction, disclosure or modification of hardware, software, networks and/or data.

This security policy has been written to specifically address the security of data used by the Payment Card Industry.

Credit card data stored, processed or transmitted by Cumberland County must be protected and security controls must conform to the Payment Card Industry Data Security Standard (PCI DSS).

III. DEFINITIONS

In addition to any other definitions set forth elsewhere in this policy, the following words when initially capitalized shall have the following meanings:

A. "Application" means all programs or groups of programs, including both internal and external (for example, web) applications, which is used by or contained on any particular portion of a computer system.

B. "Cardholder Data" means data concerning a payment card consisting of Sensitive Card Data, the cardholder name, the card expiration date and/or Service Code.

C. "Cardholder Data Environment" means the people, processes and technology that store, process, or transmit Cardholder Data.

D. "Cardholder Data Network" means that portion of the County Network which handles, processes, stores, transmits, acts as a conduit for, or contains Cardholder Data.

E. "Card Verification Code" means: (a) a number or code on a payment card (typically a credit or debit card) separate from the PAN; and/or (b) a data element separate from the PAN on a payment card's magnetic stripe that uses secure cryptographic processes to protect data integrity on the stripe, and reveals any alteration or counterfeiting.

F. "County Network" means any Network between two or more two or more computers or other computing hardware devices, which are part of the County System.

G. "County System" means all computers, laptops, servers, computer chips, tablets, disk, hard-drive, thumb drive , or other data storage system, device or medium, leased, owned, used, or operated by, or in the possession of, the County. The "County System" also includes, but is not limited to, the following:

1. All equipment or devices leased, owned, used, operated, or in the possession of the County which is or may be utilized to permit communications or which connects or is connected, either physically or electronically, with any of the foregoing; and
2. Any County computer system network;
3. Any computer, laptop, tablet, disk, hard-drive, thumb drive, or other storage device or medium that the County provides to an employee, contractor or other party,
4. All software, applications, and data contained on or used, stored, processed, or transmitted by any of the foregoing;

H. "Cumberland County" or "County" shall mean Cumberland County, a body politic duly existing under the laws of the State of Maine.

I. "DMZ" shall mean a physical or logical sub-network that provides an additional layer of security to the County's Network. The DMZ adds an additional layer of Network security between the Internet and the County's Network so that external parties only have direct connections to devices in the DMZ rather than the entire County network.

J. "Network" means two or more computers or other computing hardware devices that are linked together through communication channels to facilitate communication and resource sharing among a range of users of one or more individual computers or other computer hardware forming a part of that network.

K. "PAN" means the primary account number embossed and/or encoded on a payment card (typically a credit or debit card) which identifies the issuer and the particular cardholder account.

L. "PCI DSS" means the Payment Card Industry Data Security Standard developed and maintained by the Payment Card Industry Security Standards Council, version 3.0.

M. "PIN" means the "personal identification number", which is a secret numeric password known only to the user and a system to authenticate the user to the system. The user is only granted access if the PIN the user provided matches the PIN in the system. Typical PINs are used for automated teller machines for cash advance transactions. Another type of PIN is one used in EMV chip cards where the PIN replaces the cardholder's signature.

N. "PIN Block" means a block of data used to encapsulate a PIN during processing. The PIN block format defines the content of the PIN Block and how it is processed to retrieve the PIN. The PIN Block is composed of the PIN, the PIN length, and may contain a subset of the PAN.

O. Sensitive Authentication Data" means security-related information (including but not limited to Sensitive Card Data, full track data (from the magnetic stripe or equivalent on a chip), used to authenticate cardholders and/or authorize payment card transactions.

P. "Sensitive Card Data" means the PAN, Card Verification Code (CID, CAV, CAV2, CVC, CVV, CVV2, CVC, CVC2, CSC), any other form of magnetic stripe data from the card (Track 1, Track 2), and any PIN or PIN Block.

Q. "Service Code" means a three-digit or four-digit value in the magnetic-stripe of a payment card that follows the expiration date of the payment card on the track data. It is used for various things such as defining service attributes, differentiating between international and national interchange, or identifying usage restrictions.

R. "Strong Cryptography" means cryptography based on industry-tested and accepted algorithms, along with strong key lengths (minimum 112-bits of effective key strength) and proper key-management practices. Cryptography is a method to protect data and includes both encryption (which is reversible) and hashing (which is not reversible, or "one way").

S. "Trusted Network" shall mean the County Network, except as otherwise provided in the definition of an "Untrusted Network".

T. "Untrusted Network" shall mean:

1. Networks other than the County Network,
2. Networks which are outside of Cumberland County's ability to control or manage (e.g., the Internet, connected vendor networks, public wireless networks); and

3. With respect to traffic between any segment or part of the County Network which is used for the storing, processing, or transmitting of sensitive data with any other segment or part of the Any lower security segment or part of the County Network that is used for normal business purposes, but which is not used for the storing, processing, or transmitting of sensitive data to the extent of any traffic between that part or segment and another part or segment of the County Systems which is used for normal business purposes, but which is not used for the storing, processing, or transmitting of sensitive data.

IV. SECURITY POLICY OWNERSHIP AND RESPONSIBILITIES

It is the responsibility of the custodians of this security policy to publish and disseminate these policies to all users of the County System (including vendors, contractors, and business partners). Also, the custodians must see that the security policy addresses and complies with all standards Cumberland County is required to follow (such as the PCI DSS). This policy document will also be reviewed at least annually by the custodians (and any relevant data owners) and updated as needed to reflect changes to business objectives or the risk environment.

Questions or comments about this policy should be directed to the custodians of this policy as detailed in Table 1. Please note that Cumberland County may modify this Table at any time and that users should ensure that they have the most recent version of this Table.

Table 1 – Security Policy Custodians

Name	*Title*	*Phone*
Aaron Gilpatric	Director of IT	207-774-1444
Alex Kimball	Director of Finance	207-699-1988

V. BUILD AND MAINTAIN A SECURE NETWORK INFRASTRUCTURE

To protect sensitive and/or confidential data, it is critical to design and maintain a secure network infrastructure where this data may be stored, processed, or transmitted.

The following polices cover the network infrastructure (hardware such as firewalls, routers, and switches) as well as requirements for the secure configuration of all County System components (network hardware, servers, workstations, etc.).

1.0 Install and Maintain a Firewall Configuration

Firewalls are computer devices (either hardware or software) that control computer traffic allowed between an entity's Network (internal) and untrusted Networks (external), as well as traffic into and out of more sensitive areas within an entity's internal trusted network.

A firewall examines all traffic into and out of a Network, as well as into and out of more sensitive areas of a Network from and to other parts of that same Network, and blocks those transmissions that do not meet specified security criteria.

All systems must be protected from unauthorized access from untrusted Networks, whether entering the system via the Internet as e-commerce, employees' Internet access through desktop browsers, employees' e-mail access, dedicated connections such as business to business connections, via wireless networks, from less secure to more secure Network segments on an internal Network, or via other sources. Often, seemingly insignificant paths to and from untrusted Networks can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer Network.

1.1 Firewall/Router Configuration Documentation

Cumberland County will have documented Firewall/Router configuration standards that include the following:

- A firewall must be present between each "public" Network segment and the Cardholder Data Network. Public Network segments would include the Internet or any other County "out-of-scope" Intranet segments (i.e. less secure internal County segments where credit card data is not stored, processed, or transmitted). (PCI-DSS Requirement 1.1.4)
- Firewall configuration documentation must contain a description of the groups and/or individuals responsible for logical management of the firewalls/routers, as well as their roles and responsibilities. (PCI-DSS Requirement 1.1.5)
- Firewall configuration documentation must contain a detailed list of inbound and outbound services, protocols, and ports required for daily business. This list must contain a description and justification for use of the required services, protocols, and ports on all firewall interfaces. (PCI-DSS Requirement 1.1.6)

1.2 Restrict Connections Between Untrusted Network Segments and the Cardholder Data Environment

Cumberland County will restrict connections from Untrusted Networks to the Trusted Network within the cardholder data environment by doing the following:

- Firewall rules must limit all inbound and outbound traffic to/from the Cardholder Data Network to only that which is necessary for the business being transacted with that cardholder. (PCI-DSS Requirement 1.2.1b)
- When wireless networking is used, require a firewall between any wireless network and the cardholder data environment. Firewall rules must deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the Cardholder Data Environment. (PCI-DSS Requirement 1.2.3)

1.3 Prohibit Direct Public Access between the Internet and the Cardholder Data Environment

Cumberland County will prohibit direct public access between the Internet and any system component in the Cardholder Data Environment by doing the following:

- Create a DMZ (using appropriate firewall configuration) to limit inbound and outbound traffic to only protocols that are necessary for the Cardholder Data Environment. (PCI-DSS Requirement 1.3.1)
- Limit all inbound traffic to from the Internet to addresses within a DMZ. (PCI-DSS Requirement 1.3.2)
- Direct network routes and connections are prohibited (inbound or outbound) between the Internet and the Cardholder Data Network. (PCI-DSS Requirement 1.3.3)
- Implement anti-spoofing measures, including, for example, ensuring that internal IP addresses (e.g., RFC 1918 address ranges) do not pass from the Internet into the DMZ. (PCI-DSS Requirement 1.3.4)
- Outbound traffic from any Cardholder Data Environment zone must be explicitly authorized (PCI-DSS Requirement 1.3.5)
- Use firewall hardware that implements stateful inspection, also known as dynamic packet filtering. (That is, only "established" connections are allowed into the network, and even then only if they are associated with a previously established session.) (PCI-DSS Requirement 1.3.6)
- Hide the structure of the County Network from the Internet using technologies such as NAT, PAT, RFC 1918 address space, etc. (PCI-DSS Requirement 1.3.8)

1.4 Personal Firewall Required on Mobile Computers

- Personal firewalls must be installed and active on all mobile devices which are part of the Network or are owned by employees of the County, and/or employee-owned devices, with direct connectivity to the Internet (for example, laptops used by employees), and which are used to access the Cardholder Data Network. (PCI-DSS Requirement 1.4a)
- Personal firewall software is to be configured by Cumberland County to specific standards and is not alterable by mobile computer users. (PCI-DSS Requirement 1. 4a)

2.0 Change Vendor-supplied Defaults

System components used in sensitive networks often will come with default vendor settings (usernames, passwords, configuration settings, etc.). Cumberland County's general policy is to always change vendor-supplied defaults for system passwords or other security parameters before components become part of the County Network.

Individuals with malicious intent (external and internal to a company) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known by hacker communities and are easily determined via public information.

2.1 Change Vendor-supplied Defaults

- All vendor-supplied defaults must be changed on all components before becoming part of the County Network. (Examples include defaults used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, passwords, simple network management protocol (SNMP) community strings, etc.) (PCI-DSS Requirement 2.1)
- All default settings for wireless environments (equipment) connected to the Cardholder Data Environment or transmitting Cardholder Data must be changed before enabling the wireless system for production use. (PCI-DSS Requirement 2.1.1)
- Require that all wireless devices be configured to support strong encryption technologies (i.e. WPA/WPA2) for both authentication to the County Network and transmission of data. (PCI-DSS Requirement 2.1.1)

2.2 Remove Unnecessary Functionality

- All unnecessary functionality or software is to be removed from system components in the Cardholder Data Network. (PCI-DSS Requirement 2.2.5)

2.3 Use Secure Protocols for Non-Console Access

- Strong Cryptography must be used for any non-console and/or web-based management interface used for administration of systems and/or system components. (Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.) (PCI-DSS Requirement 2.3)

VI. PROTECT SENSITIVE DATA

Sensitive and/or confidential data (e.g., Cardholder Data) must be protected when stored and when it is in transit over Untrusted Networks. Strong industry standard encryption methodologies must be used to protect data stored on hard drives, removable media, backups, etc. The following policies ensure proper encryption of stored data and data in transit over open, public networks.

3.0 Protect Stored Data

Protection methods such as encryption, truncation, masking, and hashing are critical components of sensitive data protection. If an intruder circumvents other County Network security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable.

3.1 Storage of Sensitive Credit Card Account Number

- Never store Sensitive Card Data such as the PAN on any component of the County System unless absolutely necessary for legal, regulatory, or business purposes. (Required if using SAQ C form).

3.2 Storage of Sensitive Credit Card Authentication Data

- Never store Sensitive Authentication Data, such as the authentication data (Track, CVC, PIN), after an authorization event has taken place (even if encrypted). (PCI-DSS Requirement 3.2).
- Never store the full contents of any track from the magnetic stripe (located on the back of a card, contained in a chip, or elsewhere) on the System after any type of card authorization event. (PCI-DSS Requirement 3.2.1).
- Never store the Card Verification Code data (3 or 4 digit number located on the back or front of the customer's plastic card) on the System after any type of card authorization event. (PCI-DSS Requirement 3.2.2).
- Never store the cardholder's PIN or encrypted PIN Block data on the County System after any type of card authorization event. (PCI-DSS Requirement 3.2.3).

3.3 Mask Credit Card Numbers in Displays Wherever Possible

- All PANs will be masked or truncated when displaying card numbers on any media such that only personnel with a legitimate business need can see the full PAN. (PCI-DSS Requirement 3.3)

4.0 Encrypt Transmission of Data Over Public Networks

Sensitive information must be encrypted during transmission over Networks that are easily accessed by individuals with malicious intent. Improperly configured wireless networks and vulnerabilities in legacy encryption and authentication protocols can be continued targets of individuals with malicious intent who exploit these vulnerabilities to gain privileged access to sensitive data environments.

4.1 Transmission of Card Data Over Public Networks

- Strong encryption algorithms and protocols (ex: SSL/TLS, IPSEC) must be used whenever Cardholder Data is transmitted or received over open, public Networks. (PCI-DSS Requirement 4.1).
- Any wireless systems used in the card network must prohibit the use of the WEP protocol. (PCI-DSS Requirement 4.1.1).

4.2 Transmission of Card Data Via End User Messaging Technologies

- Prohibit the transmission of unencrypted Cardholder Data via end-user messaging technologies (e.g., e-mail, instant messaging, etc.). (PCI-DSS Requirement 4.2).

VII. MAINTAIN A VULNERABILITY MANAGEMENT PROGRAM

System components within the sensitive data environment (Cardholder Data Network) must be part of an active vulnerability maintenance program. This program will control the existence of malicious software (e.g., anti-virus software) and provide policies covering development efforts and system or software updates/upgrades such that security is maintained.

The following policies ensure system components are protected from malicious software and vulnerabilities that result from software bugs and improperly patched applications and operating systems.

5.0 Use Regularly Updated Anti-Malware Software

Malicious software, commonly referred to as "malware"—including viruses, worms, and Trojans—enters a sensitive Network segment during many business approved activities including employees' e-mail and use of the Internet, mobile computers, and storage devices, resulting in the exploitation of system vulnerabilities. Anti-virus software must be used on all systems commonly affected by malware to protect systems from current and evolving malicious software threats. Additional anti-malware solutions may be considered as a supplement to the anti-virus software; however, such additional solutions do not replace the need for anti-virus software to be in place.

5.1 Use Anti-Virus Software to protect Systems

- Anti-virus software must be deployed on all portions of the County System that are commonly affected by malicious software. This includes personal computers, servers, etc. that are attached to the segment of the County Systems which deal with or contain Cardholder Data. (PCI-DSS Requirement 5.1).
- Anti-virus programs must capable of detecting, removing, and protecting against all known types of malicious software (adware, spyware, etc.). (PCI-DSS Requirement 5.1.1).

5.2 Use Anti-Virus Software to protect Systems

- All anti-virus software and its associated definition files are to be kept up-to-date at all times. (PCI-DSS Requirement 5.2a).
- All anti-virus software must be actively running, configured to perform automatic updates and periodic scans, and capable of generating audit logs. (PCI-DSS Requirement 5.2bc, & d).
- Anti-virus software audit logs must be retained for one year. (PCI-DSS Requirement 5.2d).
- Anti-virus software must be configured so that it cannot be disabled or altered by users, except where there is a legitimate technological need for that software to be temporarily disabled as formally authorized by County management on a case-by-case basis. (PCI-DSS Requirement 5.3).

6.0 Develop and Maintain Secure Systems and Applications

Individuals with malicious intent use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities can be fixed by applying vendor-provided security patches. All systems must have all appropriate software patches to protect against exploitation and compromise of sensitive data (including Cardholder Data) by malicious individuals and malicious software.

6.1 Regularly Update Systems and Software

- All County System components and software must have the latest vendor-supplied system security patches installed. (PCI-DSS Requirement 6.2).
- All critical system and software patches must be installed within 30 days of vendor release. (PCI-DSS Requirement 6.3.b).

6.2 System Administrator Duties

- System administrators are to subscribe to outside sources for security vulnerability information and that system configuration standards are to be reviewed and updated as new vulnerability information might dictate. Outside sources might include SecurityFocus, A/V companies, SANS, CIS, Secunia, Microsoft, etc. (PCI-DSS Requirement 6.1.b).

6.3 Protect Exposed Web Applications

- All publicly exposed web applications used store, process, or transmit Card Data must be protected by an automated technical solution that detects and prevents web-based attacks (for example, a web application firewall) in front of those applications to continually check all traffic. (PCI-DSS Requirement 6.6).

VIII. IMPLEMENT STRONG ACCESS CONTROL MEASURES

Access to system components and software within the sensitive data environment (Cardholder Data Network) must be controlled and restricted to those with a business need for that access. This is achieved through the use of active access control systems, strong controls on user and password management, and restricting physical access to critical or sensitive components and software to individuals with a "need to know".

7.0 Restrict Access to Sensitive Data

Systems and processes must be in place to limit access to critical data and systems based on an individual's need to know and according to job responsibilities.

"Need to know" means that an individual's access rights will be granted only for access to the least amount of data and privileges needed to perform that individual's job for the County.

7.1 Restrict Access to Systems in Cardholder Data Environment

- Access to Cardholder Data and the portion of the County's System handling Cardholder Data must be restricted by business need to know. (PCI-DSS Requirement 7.1).
- Automated role based access control systems must be in place on all portions of the County System which handle, process, or contain Cardholder Data. User ID's must limit users rights to only those necessary for their job classification and function. (PCI-DSS Requirement 7.1.2).

8.0 Assign a Unique ID to Access System Components

It is critical to assign a unique identification (ID) to each person with access to critical systems or software. This ensures that each individual is uniquely accountable for his or her actions. When such accountability is in place, actions taken on critical data and systems are performed by, and can be traced to, known and authorized users.

8.1 Require Unique User IDs

- Unique IDs will be assigned to all users before they will be permitted to access System components in the Cardholder Data Environment. (PCI-DSS Requirement 8.1.1).

8.2 Password Reset

- All non-face-to-face password reset requests for users with access to the Cardholder Data Network require a verification of employee identity. (PCI-DSS Requirement 8.2.2).

8.3 Vendor Management Accounts

- Vendor accounts for remote or on-site maintenance are only enabled during the time period needed by the vendor and monitored by Cumberland County employee while being used. (PCI-DSS Requirement 8.1.5).

8.4 Password Reset

- Use of group or shared User IDs or passwords is specifically prohibited. (PCI-DSS Requirement 8.5).

9.0 Restrict Access to Sensitive Data and System Components

Any physical access to data or systems that house sensitive data (Cardholder Data) provides the opportunity for individuals to access devices or data and to remove systems or hardcopies, and should be appropriately restricted.

9.1 Securing Hard Copy Materials

- Cumberland County will define procedures required for physically securing paper and hard copy materials (which includes paper receipts, mail, reports, and faxes), as well as all other media, containing Cardholder Data within all facility locations. (PCI-DSS Requirement 9.5).

9.2 Secure Media Containing Sensitive Data

- Cumberland County will define specific procedures required for controlling the internal or external distribution of any kind of media containing cardholder data. It will maintain strict control over the storage and accessibility of both hardcopy and electronic media that contains cardholder data. (PCI-DSS Requirement 9.6, 9.7)
- Media must be classified and labeled in such a way that it can be identified as “Confidential”. (PCI-DSS Requirement 9.7.1)

- All media containing sensitive Cardholder Data sent outside the facility must be transferred by secured courier or other delivery method that can be accurately tracked. All transfers of media containing Cardholder Data will be logged. Logs must show management approval, and tracking information. Retain media transfer logs. (PCI-DSS Requirement 9.6.2)
- Management approval is required prior to moving any and all media containing Cardholder Information out of a secured area (especially when media is distributed to individuals). (PCI-DSS Requirement 9.6.3)
- Periodic inventory of stored media containing cardholder data must be performed and documentation must be retained showing these inventories were performed. (PCI-DSS Requirement 9.9)

9.3 Media Destruction Policies

- Media containing Cardholder Data must be destroyed when it is no longer needed for business or legal reasons. (PCI-DSS Requirement 9.8).
- Cumberland County must define and document specific procedures that will be used to destroy any hard copy materials containing cardholder data beyond reconstruction. Technologies such as shredding, incineration, pulping, etc. must be used to destroy media. (PCI-DSS Requirement 9.8.1).

IX. REGULARLY MONITOR/TEST SENSITIVE DATA NETWORKS

Important components of overall system security are the regular testing of networks for exposed vulnerabilities and the continuous monitoring of security indicators (logs, system events, etc.). The following policies address system monitoring and vulnerability testing.

10.0 Track and Monitor Access to Network Resources/Data

Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult without system activity logs.

10.1 Monitor System Components Within the Cardholder Data Network

- Enable audit trails (active system tracking logs) on all System components within the Cardholder Data Network (e.g., server event logs, web server logs, firewall logs, payment application logs, etc.). (PCI-DSS Requirement 10.1).
- Retain audit trail logs for 12 months. (PCI-DSS Requirement 10.7).

11.0 Regularly Test Security Systems and Processes

Vulnerabilities are being discovered continually by malicious individuals and researchers, and being introduced by new software. System components, processes, and custom software must be tested frequently to ensure security controls continue to reflect a changing environment.

11.1 Rogue Wireless Network Detection

- A wireless analyzer must be used at least quarterly to detect unauthorized wireless networks/devices within the Cardholder Data Network. (PCI-DSS Requirement 11.1)

11.2 Vulnerability Assessment Scans

- Internal vulnerability assessment scans must be performed at least quarterly and after any significant change in the Cardholder Data Network (e.g., changes in firewall rules, or upgrades to products within the environment, etc.). (PCI-DSS Requirement 11.2)
- External vulnerability scans are to be performed at least quarterly and after any significant change in the Cardholder Data Network (e.g., changes in firewall rules, or upgrades to products within the environment, etc.). An Approved Scanning Vendor (ASV) must conduct all scans. Scans must be run on all external IP addresses that could be used to gain access to the cardholder data environment. (PCI-DSS Requirement 11.2)
- Systems failing a vulnerability assessment scan (either internal or external) are to be remediated and retested until a passing scan is achieved. (PCI-DSS Requirement 11.2)
- Results of each quarter's internal and external vulnerability assessments are to be documented and retained for review. (PCI-DSS Requirement 11.2)

X. MAINTAIN AN INFORMATION SECURITY POLICY

Without strong security policies and procedures many of the layers of security controls become ineffective at preventing data breech. Unless consistent policy and practices are adopted and followed at all times, security controls break down due to inattention and poor maintenance. The following documentation policies address maintaining the Cumberland County security policies described above.

12.0 Maintain a Security Policy for Employees and Contractors

---

A strong security policy sets the security tone for Cumberland County and informs employees and vendors what is expected of them. All employees and vendors should be aware of the sensitivity of data and their responsibilities for protecting it.

12.1 Publish the Information Security Policy

- Cumberland County requires that the most recent version of the information security policy be published and disseminated to all relevant system users (including vendors, contractors, and business partners). (PCI-DSS Requirement 12.1)
- The Cumberland County information security policy must be reviewed at least annually to keep it up to date with changes in the industry and with any changes in the cardholder network environment. (PCI-DSS Requirement 12.1.1)

12.2 Employee Facing Technologies

- The use of the following technologies are prohibited: remote-access technologies, wireless technologies, removable electronic media, laptops, tablets, e-mail usage, chat usage, and Internet usage.

- Any exception to this requirement must be explicitly requested and approval given in writing that includes acceptable use of the technology and locations to be used from.
- Any allowed technology must use authentication with username & password or tokens.
- The allowed devices & personnel must be documented and labeled.
- Remote access technologies must be configured to time out after 10 minutes of inactivity. Remote access for vendors and business partners will only be activated when needed and immediately deactivated after use.(PCI-DSS Requirement 12.3)

12.3 Assign Information Security Responsibilities & Train Employees

- The Cumberland County's information security policy and procedures must clearly define the information security responsibilities of both employees and contractors. (PCI-DSS Requirement 12.4)
- Responsibilities of information security at Cumberland County must be formally assigned to a specific individual(s), position, or team. (PCI-DSS Requirement 12.5)
- Specifically the following responsibilities must be formally assigned to a specific individual(s), position, or team (see Appendix A):
  - Responsibility for establishing, documenting, and distributing the Cumberland County information security policies and procedures. (PCI-DSS Requirement 12.5.1)
  - Responsibility to monitor, analyze, and distribute security alerts and information. (PCI-DSS Requirement 12.5.2)
  - Responsibility to establish, document, generate, and distribute detailed documentation security incident response and escalation procedures. (See Appendix B) (PCI-DSS Requirement 12.5.3)
  - Responsibility to administer users in the Cardholder Data Network. Includes all additions, deletions and modifications to user access. (PCI-DSS Requirement 12.5.4)
  - Responsibility to monitor and control all access to Cardholder Data. (PCI-DSS Requirement 12.5.5)
- A formal security awareness program must be created and implemented, and participation is required for all employees working within the Cardholder Data Environment. (PCI-DSS Requirement 12.6).

12.4 Policies For Sharing Data With Service Providers

If Cardholder Data is shared with service providers (for example, back-up tape storage facilities, managed service providers such as Web hosting companies or security service providers, or those that receive data for fraud modeling purposes), the following policies and procedures must be followed:

- Cumberland County must maintain a documented list of any service provider that is given access to Cardholder Data, provided direct access to the Cardholder Data Network, or can affect the security of the Cardholder Data Network. (PCI-DSS Requirement 12.8.1).
- Any written agreement with a service provider that is given access to Cardholder Data, provided direct access to the Cardholder Data Network, or can affect the security of the Cardholder Data Network, must include an acknowledgement of the service provider's responsibility for securing all Cardholder Data they receive from Cumberland County or

which they access, as well as to the extent that they could impact the Cardholder Data Environment. (PCI-DSS Requirement 12.8.2).

- Prior to engaging with a service provider that is given Cardholder Data, provided direct access to the Cardholder Data Network, or can affect the security of the Cardholder Data Network, Cumberland County will conduct due diligence and follow an established process to ensure that the security of Cardholder Data within the service provider's Network, or which the service provider may obtain or obtain access to, has been addressed. (PCI-DSS Requirement 12.8.3).
- Cumberland County will have an ongoing program to monitor the PCI DSS compliance status of any service provider that is given access to Cardholder Data, provided direct access to the Cardholder Data Network, or can affect the security of the Cardholder Data Network. (PCI-DSS Requirement 12.8.4)

XI. ATTACHMENTS

Appendix C1: *Management Roles and Responsibilities*
Appendix C2: *Incident Response Policy*
Appendix C3: *Agreement to Comply*

#7: Surplus Material & Sale of County Property

I. SURPLUS MATERIAL

All using departments shall submit to the Facilities Department, reports showing stocks of all supplies and equipment which are no longer used or which have become obsolete, worn out or scrapped.

A. Transfer. The Facilities Director shall have the authority to transfer surplus stock to other using departments.

B. Municipal Transfer. The Facilities Department will periodically circulate a list of unwanted surplus material to municipalities in Cumberland County. The Facilities Department will invite inquiries for a 45-day period.

C. Sale. The Facilities Department, after offering to municipalities, shall have the authority to sell all supplies and equipment, not taken by county departments or municipalities. Sale of surplus property shall be accomplished by a competitive bidding procedure, an open sale or auction. The Facilities Director, with the approval of the County Manager, shall determine the type of sale. Supplies or equipment not sold within sixty (60) days of being offered may be deemed by the Facilities Director to have no value and be disposed of in an appropriate environmental manner.

1. Competitive bidding. In cases where the value of an item warrants a competitive bidding process, sales under the competitive bidding procedure shall be made to the highest bidder. The Facilities Director shall have the authority to award bids, provided the Commissioners shall approve all awards of bid of ten thousand dollars ($5,000.00) or more.
2. Open sales may be electronic, and the Facilities Director may create a continuous electronic auction to which new supplies and equipment are added as deemed appropriate. The use of on-line auction sites or sites similar to Craigslist/Maine shall be an acceptable use of sale for those items not requiring a formal competitive bid.
3. Auction. The Facility Department may periodically participate in a local/regional auction of surplus supplies and equipment. The date and location of such auctions shall be published in a newspaper of general circulation and shall be publicized in any other manner, which will be likely to inform the public of the pending event.

D. Computer Hardware & Air Conditioners. Computer hardware and/or Air Conditioners taken out of service may be offered for sale to County employees (other than the Facilities Director and Director of Information Technology) in a manner determined by the County Manager. The Facilities Director and the Director of Information Technology shall determine a reasonable market value of the items in an "as is, where is" condition, and the Facilities Director shall try and sell the items for at least that amount.

E. Disposition of Unwanted/Unclaimed Surplus.

1. Material that remains after departmental posting, municipal posting, and auction and/or public bid shall be classified as scrap.
2. Scrap material should be recycled, sold, or donated to charity if possible.
3. Material that cannot be recycled, sold, or given to charity should be-disposed of in a safe environmental way.
4. Completely unwanted material can be thrown away.

II. EXCEPTIONS

A. UNCLAIMED EVIDENCE: Evidence must be disposed of by statute, which outlines notification requirements, advertisements, and proper handling procedures.

B. SURPLUS WEAPONS: Weapons cannot be sold. Some weapons must be destroyed, but others can be used by the Sheriff's Department for trade with other law enforcement agencies. In Cumberland County, weapon disposal is the responsibility of the Sheriff.

C. SPECIALIZED POLICE EQUIPMENT: Material unique to law enforcement should be managed and scrapped by the Sheriff's Department (i.e. radar, radios, light bars, sirens, loudspeakers, etc.). Whenever possible this equipment should be handled as outlined in this policy.

D. COMPUTER EQUIPMENT: Computer equipment should be handled in consultation with the County's Information Technology Director. If the Information Technology Director recommends surplusing equipment, it is handled by the Facilities Department as outlined in this policy.

E. GRANT MATERIAL: Equipment that is acquired through grants will be surplused in accordance with applicable guidelines.

F. SPECIAL CIRCUMSTANCES: The County Commissioners and the County Manager retain complete discretion over all material owned or used by County Departments.

III. CONCLUSION

Surplus material represents an expenditure of public resources, so the County is committed to recouping public funds from surplus material wherever possible. County interests are best served by reusing, auctioning, selling, recycling or donating material that is surplus, but serviceable. It should be understood that some items are past their useful life and the efforts of staff might outweigh the value of the item. Discretion needs to be applied.

IV. SALE OF COUNTY PROPERTY.

General policy. The sale of all real property owned by the County, including any interests therein, shall be governed by this section. As a general rule, the County shall charge fair market value for the conveyance of any interest in real property, except as specifically provided below, and convey its interest by quit claim deed.

A. Any proposed sale of "county-owned" property shall first be referred to the Commissioners for its recommendation as to the disposition thereof.

B. The Commissioners shall decide whether to sell such property. If the Commissioners decides to offer the property for sale, the Commissioners shall determine the method of sale/transfer. Methods may include, but are not limited to, sealed bid, sealed request for proposals, auction, brokerage sale or negotiated sale or trade.

C. In evaluating the proposals to purchase such property, depending on the method of sale, the Commissioners may consider factors such as price, annual property tax generation, proposed land use, economic benefit, job creation, environmental benefit or detriment, historical or architectural significance of any existing improvements on the property, or community need when awarding the sale.

D. The Commissioners may set reasonable conditions on the future use of the property through deed restrictions to ensure that the property will be used in the best interests of the County.

V. ACQUISITION OF SURPLUS PROPERTY

County operations relies on a number of pieces of equipment to accomplish county operations and functions. Acquisition of new equipment falls under the County's annual bonding / non-debt Capital planning budget. Periodically, departments find a piece of equipment that serves their needs through Local, State or Federal surplus equipment list. The ability to obtain equipment from these lists is worthy, if deemed appropriate and provides a cost savings. Staff shall recognize these pieces of equipment are on surplus list for a reason, and staff should be aware and be ready to justify any costs associated with repairs, rehabilitation or rebuilding of acquired equipment. This justification shall be part of the initial review prior to acquisition.

Acquisition of surplus equipment shall abide by the following guidelines:

1. An estimated value of $10,000 or less, Department Head authorization
2. An estimated value between $10,001 and $50,000 County Manager authorization; and
3. Any estimated value over $50,001 shall seek recommendation by the County Manager and acceptance by the County Commissioners

#8: Acceptable Use of County Computer Systems, Internet and Email

I. OVERVIEW

The intention for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Cumberland County's established culture of openness, trust and integrity. Cumberland County is committed to protecting it's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of Cumberland County. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations.

Effective security is a team effort involving the participation and support of every Cumberland County employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

II. PURPOSE

The purpose of this policy is to outline the acceptable use of computer equipment at Cumberland County. These rules are in place to protect the employee and Cumberland County. Inappropriate use exposes Cumberland County to risks including virus attacks, compromise of network systems and services, and legal issues.

III. SCOPE

This policy applies to the use of information, electronic and computing devices, and network resources to conduct Cumberland County business or interact with internal networks and business systems, whether owned or leased by Cumberland County, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at Cumberland County and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with Cumberland County policies and standards, and local laws and regulation. Exceptions to this policy are documented in section 5.2

This policy applies to employees, contractors, consultants, temporaries, and other workers at Cumberland County, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Cumberland County, including employees who may remotely access the network from home.

IV. POLICY

A. General Use and Ownership

1. All material created, modified, stored, distributed, transferred, printed, imaged, or otherwise processed on the County's automation equipment is considered to be public property and, as such, is subject to examination by the public, except as noted below:
   a) All of this information may be subject to release under a "Freedom of Access Law" request. The State of Maine "Freedom of Access Law" (1 MRSA, § 401-410) provides that any and all materials, files, notes, records, and copies regardless of the media used to store or transmit them (paper, film, microfiche, magnetic media, or electronic media) in public offices or in the possession of public employees while at work which relate in any way to the transaction of governmental business are public property. As such, the public has access to those materials.
   b) The law places very narrow restrictions on public access to such materials as personnel files, employment applications, employee testing and rating criteria workers' compensation files, and certain investigation files. Most materials, however, are subject to Freedom of Access requests.
2. You may access, use or share Cumberland County proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties. You have a responsibility to promptly report the theft, loss or unauthorized disclosure of Cumberland County proprietary information.
3. Employees should only use County provided equipment and Internet services for County related activities and may not use their service for personal business. Employees are responsible for exercising good judgment regarding the reasonableness of personal use, and if there is any uncertainty, employees should consult their supervisor or manager.
4. Employees should remember that existing rules, regulations, and guidelines on ethical behavior of County employees, and the appropriate use of County resources, apply to the use of electronic communications systems supplied by the County of Cumberland.
5. Employees are advised that they should have no expectation of privacy when using County computer equipment, including E-Mail or the Internet. E-mail messages and Internet sites accessed or stored on County equipment are not private, but are property of Cumberland County. For security and network maintenance purposes, authorized individuals within Cumberland County may monitor equipment, systems and network traffic at any time.
6. Cumberland County reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

B. Security and Proprietary Information

1. System level and user level passwords must comply with the *Password Policy*. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.
2. All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 30 minutes or less. You must lock the screen or log off when the device is unattended.

3. Postings by employees from a Cumberland County email address to newsgroups, or social media, should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Cumberland County, unless posting is in the course of business duties.
4. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

C. Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of Cumberland County authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Cumberland County-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

1. **System and Network Activities**

   The following activities are prohibited:

   a) Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Cumberland County.

   b) Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Cumberland County or the end user does not have an active license is strictly prohibited.

   c) Use of County equipment to view offensive materials on the basis of race, ethnicity, religious beliefs, disability, sexual orientation, age, gender, and/or materials that are sexually oriented, explicit, or pornographic in nature is prohibited.

   d) Accessing data, a server or an account for any purpose other than conducting Cumberland County business, even if you have authorized access, is prohibited.

   e) Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

   f) Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

   g) Online activities that consume large amounts of bandwidth, and subsequently impact network performance for business functions, are prohibited. This includes, but is not

limited to, streaming video or audio, listening to internet radio, online game playing, and downloading excessive large files.

h) Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

i) Using a Cumberland County computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

j) Making fraudulent offers of products, items, or services originating from any Cumberland County account.

k) Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

l) Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

m) Port scanning or security scanning is expressly prohibited unless prior notification to IT is made.

n) Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

o) Circumventing user authentication or security of any host, network or account.

p) Introducing honeypots, honeynets, or similar technology on the Cumberland County network.

q) Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

r) Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

s) Providing information about, or lists of, Cumberland County employees to parties outside Cumberland County.

t) The storage of any credit card numbers or identifiable information on any County owned equipment.

2. Email and Communication Activities

When using company resources to access and use the Internet, users must realize they represent the company. Whenever employees state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company". Questions may be addressed to the IT Department

a) All use of email or instant messaging must be consistent with County policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices.

b) County email account should be used primarily for business-related purposes; personal communication is permitted on a limited basis, but non-County related commercial uses are prohibited. Any use for fund-raising, political or other public relations activities not specifically related to county government activities are strictly prohibited.

c) The County email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any employee should report the matter to their supervisor immediately.

d) Users are prohibited from automatically forwarding County email to a third party email system. Individual messages which are forwarded by the user must not contain confidential information.

e) All County email accounts shall use an approved email 'signature' containing the sender's name and contact information. Users are prohibited from customizing this signature with personal quotes or verbiage that reflects poorly on the County. Users must have modifications to the email signature approved by their department head prior to use.

The following activities are strictly prohibited, with no exceptions:

f) Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

g) Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

h) Unauthorized use, or forging, of email header information.

i) Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

j) Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

k) Use of unsolicited email originating from within Cumberland County's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Cumberland County or connected via Cumberland County's network.

l) Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

m) Sending credit card numbers or personally identifiable information to any recipient.

3. Blogging and/or Social Media

a) Blogging or Social Media posts by employees, whether using Cumberland County's property and systems or personal computer systems, is also subject to the terms and

restrictions set forth in this Policy. Employees may not use Cumberland County's systems to engage in blogging or social media posts unless it is required by their job duties and previously approved by their supervisor. When posting, employees must ensure that it is done in a professional and responsible manner, and does not otherwise violate Cumberland County's policy, or is not detrimental to Cumberland County's best interests. Posting from Cumberland County's systems is also subject to monitoring.

b) Cumberland County's Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any confidential or proprietary information, trade secrets or any other material covered by Cumberland County's Confidential Information policy when engaged in blogging.

c) Employees shall not engage in any posts that may harm or tarnish the image, reputation and/or goodwill of Cumberland County and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when posting online or otherwise engaging in any conduct prohibited by Cumberland County's Personnel Policy.

d) Employees may also not attribute personal statements, opinions or beliefs to Cumberland County. If an employee is expressing his or her beliefs and/or opinions online, the employee may not, expressly or implicitly, represent themselves as an employee or representative of Cumberland County. Employees assume any and all risk associated with blogging or posting social media messages online.

e) Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, Cumberland County's trademarks, logos and any other Cumberland County intellectual property may also not be used in connection with any blogging activity.

V. POLICY COMPLIANCE

A. Compliance Measurement

The IT team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

B. Exceptions

Any exception to the policy must be approved by the IT Director in advance.

C. Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

EFFECTIVE: March 11, 2019

#9: Cumberland County Courthouse

Emergency Evacuation Plan

I. PURPOSE

The intent of this emergency plan is to provide a safe working environment for Cumberland County employees, and other citizens who visit for services. This plan will include guidelines to evacuate during emergencies. The sections in this regulation provide a quick reference guide for handling some emergencies. It is not intended to be all-encompassing nor is it a substitute for common sense and due diligence where safety and security are concerned.

II. POLICY

This regulation provides the framework for employees to use in an event of an emergency, natural disaster, or man-made incident. At no time should anyone put themselves in a situation which may result in injury or the loss of life.

III. REPORTING PROCEDURES

In the event of an emergency or disaster requiring alerting emergency personnel, notify the following:

A. State Security at 822-4170 (Control Room)
B. Fire Department (911)
C. Activate the Fire Alarm system by means of a "Pull Station" located near each exit of the building.
D. Activate the duress button should you have one at your workstation.

IV. EVACUATION

A. Evacuate anyone in the immediate area and/or those in need of assistance by means of the nearest exit. Employees should become familiar with these exits.

B. Exit your office last person to leave should close but DO NOT LOCK the door.

C. Once outside of the building, proceed immediately to either the **Primary**

Evacuation Point (county garage in the portion used by Portland Police Department. It is on the farthest end of the garage away from the courthouse) or, should that be unavailable, the **Secondary Evacuation Point (Lincoln Park, in the vicinity of the fountain).**

D. Staff persons will assist in the evacuation of the facility by directing visitors or people they are working with to the nearest exit.

E. In the event that a visitor refuses to leave the building during an alarm sounding, Staff should not physically encourage the person to leave. These situations should be reported to State Security as soon as possible so it can be dealt with.

F. Do not open doors which are hot or which have venting smoke.

G. If you are surrounded by smoke, get on your hands and knees and crawl to an exit. You will inhale less smoke near the floor.

H. Once you are outside the building, NEVER re-enter the building for any reason and proceed to the designated evacuation point.

I. When you hear the alarm system activate, your immediate concern should be to evacuate the building. Do not question the alarm as to whether or not it is real or false. **All alarms are to be considered "real" until advised otherwise by the Fire Department.**

J. Employees should **NOT** use fire extinguishers unless properly trained to do so. Training will be provided to designated employees on an individual basis. The fire extinguishers that are located throughout the building are intended for egress only.

V. DEPARTMENT SUPERVISOR/MANAGER PROCEDURES

A. Any emergency or disaster requires the department head, or designated person, to notify State Security at 822-4170 and to call the Fire Department (911).

B. Once outside the building, all employees should proceed immediately to the **Primary or Secondary Evacuation Point.**

C. The department head or designated person will take a roll call and ensure everyone is accounted for. If there is someone missing, recheck with other department members to verify their last known whereabouts and then report the missing person and last known location to Security or the Safety Coordinator or Facilities Manager when he/she comes to your meeting location. Do not try to find the Safety Coordinator or Manager to report. Stay at your meeting location.

VI. TRAINING

A. All employees will receive a copy of the emergency evacuation plan from Human Resources during new employee orientation and will be responsible to answer any questions from employees as needed.

B. Emergency evacuation exercises (fire drills) will be conducted annually.

C. All employees will receive a copy of the emergency evacuation plan. Should evacuation routes or responsibilities change, all employees will receive a revised copy of these changes.

VII. EMERGENCY ALARM SYSTEM

The fire alarm system will use a distinctive signal and comply with the requirements in 29CFR1910.16.5

EFFECTIVE: March 11, 2019

#10: Cumberland County Property

I. PURPOSE

The purpose of this policy is to maintain a written record of County property issued to employees and designate responsibility for the return of property upon termination.

II. POLICY

A. County property may be issued to employees at the beginning of employment with Cumberland County as well as periodically during the course of employment.

B. Property issued includes keys, parking permit cards, building security cards, uniforms, equipment, tools and a variety of other County property pertinent to various positions and departments of County government.

C. Departments that issue property shall be responsible for the inventory maintenance of what has been issued and returned.

III. PROCEDURE

A. Upon employment, each department shall be responsible for issuing property within their own department and shall maintain an inventory of what has been issued.

B. The generated County Property list must be signed upon receipt of property and submitted to the Human Resources Director for inclusion in their personnel file.

C. Upon termination, the Human Resources Director shall verify with the appropriate department(s) all property is returned to the County prior to the issuance of the last paycheck. If property is not returned appropriate payroll deduction shall be made. The Payroll Supervisor shall verify the status of property with the Human Resources Director prior to the release of the last paycheck.

EFFECTIVE: March 11, 2019

#11: Public Health Emergencies

Human Resources Guidelines

I. PURPOSE

To provide clear, concise guidelines for leave utilization, staffing of offices, and personal hygiene in order to safeguard the health of employees and their families while continuing to provide quality service to the public during a public health emergency such as a pandemic influenza.

II. POLICY

During a period of public health emergency it is important that communication flow throughout Cumberland County Government. The Emergency Management Director will communicate to managers and department heads that are responsible for communicating operational requirements throughout their departments. When a declaration of Public Health Emergency is declared or there is a change in circumstance, The County Manager has the discretionary authority to issue different policies for time off.

A. Leave Usage

During these public health emergencies, it will be necessary for some staff to be absent from work. The following guidelines apply:

1. Sick leave can be used in accordance with collective bargaining agreements and the County Personnel Policy, which states that sick leave/earned time can be used for illness and/or medical care of the employee or a member of the employee's immediate family that requires the attention or presence of the employee.
2. Employees may request under the (FMLA) Family Medical Leave Act up to 12 weeks, if eligible. Your FMLA will be paid in accordance with Non-union Personnel Policy. Frozen sick leave may be utilized by those employees who may have a balance.
3. If your child's day care center or school is closed, and your child is not sick, you may use your accrued vacation, earned time, or personal and then unpaid leave.
4. Vacation leave, earned time will be granted if operational needs of the department and critical job function can be met based on existing staff.
5. Should office closures be necessary, essential services will continue. Administrative leave may be granted in accordance with inclement weather policies or staff may be relocated to other work locations.

B. Staff Redeployment

It may be necessary to re-deploy and train staff in areas of the county where public services must be maintained.

1. When staffing absences increase due to illness, it is important for staff to report to work as scheduled. A staff member who presents symptoms of contagious illness while at work will be sent home utilizing accrued leave. Department heads/managers

will communicate with the County Manager/ or designee prior to sending employees home.

2. Skill sets of staff will be identified to determine qualification and ability to perform the functions of other like jobs. Staff will receive necessary orientation/training from appropriate personnel prior to reassignment to another department. If an employee refuses the reassignment, options include progressive discipline, and asking for volunteers for a temporary assignment.

3. Telecommuting will be limited to certain employees with approval of the County Manager.

C. Universal Precautions

All staff are encouraged to practice good hygiene while carrying out work duties, and take necessary precautions which include:

1. Frequent hand washing, use of waterless hand sanitizer, coughing into sleeves, or tissues.

2. Vaccinations

3. Social distancing is recommended to ensure the spread of contagious illness is prevented.

4. Protective equipment will only be worn when it is provided and based upon public health recommendations such as gloves, protective eyewear, and masks.

EFFECTIVE: March 11, 2019

#12: Safety and Health Statement

I. PURPOSE

Cumberland County Government is dedicated to providing a safe and healthy environment for employees and the public.

II. POLICY

At Cumberland County Government, our most valuable resources are the people who work for us and the public we serve. Cumberland County Government is sincerely interested in our employees' safety. The policy of Cumberland County Government is to provide safe equipment, adequate tools and training, and the necessary protective equipment. An effective Safety and Health Program will be carried out throughout our organization. To achieve this objective, we will make all reasonable efforts to comply with all government regulations pertaining to safety and health issues.

Cumberland County has developed five Safety Committees, including an Executive Safety Committee, chaired by the County Safety Coordinator. Other members of the committee are representatives from each of the divisions throughout the county, including, one representative from the Communications Association Bargaining Unit. The responsibilities of the Safety Committees include analysis of data, interacting with employees and providing feedback, conducting periodic self-audits of facilities, assisting management in root cause analysis of accidents and injuries, investigations, near misses, reviewing and developing safety policies and procedures and researching and developing projects to solve problems or trends.

The Safety and Health Program will assist management and non-supervisory employees in controlling hazards and risks, which will minimize employee and public injuries and damage or destruction of Cumberland County property.

III. RESPONSIBILITIES

To accomplish our safety and health goals, all members of management are responsible and accountable for implementing this policy and ensuring that it is followed. It is also the employees' responsibility to follow the rules of safety as established for their protection and protection of others and to use the protective equipment and devices, which the County provides. All employees will follow this program. This program is designed to encourage all employees to promote the safety of their fellow employees and the public they serve.

Administrative responsibility is assigned to the Safety Coordinator. The Safety Coordinator, however, is not responsible for departmental safety, which is the responsibility of department heads and supervisors. It is expected that department heads will complement the efforts of the Safety Coordinator to reduce losses and provide for the safety of employees and the public. These loss control responsibilities are continuous and equal in importance with all other operational considerations.

Workstation ergonomic assessments will be conducted by the Safety Coordinator to ensure proper postures and ergonomic set-up in order to minimize risk of developing musculoskeletal disorders. These assessments may be requested by supervisors or managers on behalf of their staff as necessary. Employees should be encouraged to participate in assessments as well as comply with any workstation adjustments and suggestions made as a result of an assessment.

It is the responsibility of the employee to follow all safety related work rules and procedures and to cooperate with and support loss control program activities and objectives. Each employee is expected to report any unsafe conditions and to ask for instruction from a supervisor if they are unsure how to conduct a specific task safely. Employees should refer to Employee Report of Injury/Workplace Guidelines packet on the Cumberland County Intranet for injury reporting guidance.(https://sites.google.com/a/cumberlandcounty.org/ccintranet/employee-safety/employee-report-of-injury) It is the responsibility of each supervisor to monitor and assist employees in the safe performance of their duties. Safe work behaviors and attitudes are an expected part of every employee's job performance.

Loss control is every employee's responsibility. This policy statement will be reviewed annually to allow the County of Cumberland to meet the mutually beneficial goal of maintaining a safe, loss free environment for our employees.

Any unsafe conditions should be reported promptly to the immediate supervisor and appropriate Safety Committee Representative by sending an email to the Safety Coordinator or a department safety committee member.

EFFECTIVE: September 11, 2023

#13: Hazard Communication Program

I. PURPOSE

This document meets the requirements outlined in OSHA 29 CFR 1910.1200 (Hazard Communication Standard [HCS], including the updated Globally Harmonized System of Classification and Labeling of Chemicals (GHS)), and Title 26 MRSA Chapter 22 (Employee Right-to-Know [RTK]), for the development, implementation and maintenance of a written hazard communication program.

The purpose of the HazCom program is to provide information to the employees of Cumberland County regarding the identification of potential chemical and physical hazards in their workplace, the protective measures to be taken to prevent adverse effects, and their right of access to occupational health records.

II. SCOPE

The HazCom program applies to all employees of Cumberland County (including part-time employees, temporary employees, and subcontractors working onsite) who handle or use hazardous materials in the course of their work.

III. PROGRAM COMPONETS

A. Assignment of Responsibility

Each department or group will designate a Hazmat Coordinator to oversee the implementation of the HazCom program for their particular operations, specifically:

1. Obtaining Safety Data Sheets (SDS) from the manufacturer or vendor for all hazardous materials being used, handled or stored;
2. Confirming proper labeling of containers;
3. Maintaining the Chemical Inventory and the associated SDS;
4. Providing initial and annual training to employees;
5. Maintaining a HazCom Station in the workplace, for ready access to information. The station will consist of a clearly visible sign, the SDS binder for that work area, site-specific safety information (including emergency and evacuation procedures), and employee right-to-know information.

B. Chemical Inventory

All departments or groups utilizing hazardous materials must maintain an inventory of those materials, consisting of at a minimum:

1. Name and manufacturer of each material;
2. Designated area(s) of use, handling or storage;
3. Hazard determination, based on manufacturer's or vendor's information;
4. Verification of current SDS on file.

This inventory is typically in the form of an index in the front of the SDS binder. This inventory will be reviewed at least annually by the Coordinator to confirm accuracy, and to address any

out-of-date information. SDS must be retained on-file for materials no longer in use for at least 3 years.

Copies of current SDS are centralized in the Facilities office for emergency reference; in the event of a release or chemically-related injury, a copy of the appropriate SDS must accompany the employee to the medical facility.

Subcontractors working onsite must provide copies of SDS for all hazardous materials they are storing, handling or using, and comply either with the provisions of this HazCom program or their own equivalent plan.

C. Container Labeling

All hazardous materials containers will be properly labeled with the following:

1. Material name;
2. Manufacturer's name and address;
3. Physical, chemical, and health hazards of the specific material.

Original labeling from the manufacturer must contain this information, and should be used whenever possible. Properly formatted labels may also be used as replacements for unreadable original labels, and/or for secondary containers. Additional container requirements include the following:

1. All hazardous materials will be stored in the original or approved secondary container, with the label clearly visible.
2. Secondary containers include vessels being used to dispense small quantities for immediate use in the work area; unused materials must either be returned to the primary storage vessel, or disposed of as hazardous waste.
3. Secondary containers need not be separately labeled, if: (1) it is for the exclusive use of one employee; (2) no other person will have access to it; and (3) it will not be left unattended.
4. No unmarked containers may be left unattended in the work area; unmarked containers so found must be reported to the supervisor and/or Coordinator immediately, and either properly labeled, returned to its original container, or disposed of as hazardous waste.

D. Employee Training and Information

Prior to starting work, each new employee of Cumberland County will attend a safety and health orientation and will receive information and training specific to their work areas, including at least the following:

1. The provisions of the Hazard Communication Standard (HCS)and Employee Right-to-Know (RTK);
2. The location and availability of the written HazCom plan, Chemical Inventory, and SDS (HazCom station);
3. General physical, chemical and health hazards to be considered, including routes of exposure;
4. Protective measures to be taken to lesson and/or prevent adverse effects, including the use of personal protective equipment (PPE), engineering controls, and good work practices;

5. Methods and observation techniques used to determine the presence and release of hazardous chemicals in the work area.
6. Steps the County of Cumberland has taken to lessen or prevent exposure to hazardous chemicals.
7. Safety, emergency and evacuation procedures to follow if they are exposed to hazardous chemicals.
8. How to read labels and SDS; to obtain appropriate hazard information.
9. The right to access their occupational health records. A notice to this effect must be posted with the HazCom Station (example attached).

    a) After receiving training, each employee will sign a form to verify that they have received training, received written material, and understood the County policies on hazard communication.

    b) Prior to a new hazardous material being introduced into any operation, each employee will be given information as outlined above. Department Heads, in consultation with the Safety Coordinator, will ensure that SDS are available on all new chemicals.

E. Informing Contractors

It is the responsibility of the Facilities Manager or Safety Coordinator to provide contractors the information on hazardous chemicals to which they may be exposed while on the job site and precautions the employees may take to lessen the possibilities of exposure by using appropriate protective measures.

F. Distribution of SDS

The Facilities Manager or Safety Coordinator shall provide the appropriate departments with SDS when received. It is the responsibility of Department Heads to forward SDS to the Facilities Manager if received directly without being processed through Facilities.

IV. PROGRAM REVIEW

The HazCom program will be reviewed annually by the Safety Coordinator , Director of Facilities, /, and the Cumberland County Executive Safety Committee and updated as needed to maintain regulatory compliance and meet the perceived needs of the County's workplaces, at least annually.

V. ATTACHMENTS

Appendix D1*: Guidelines for Hazardous Materials and Waste Handling*
Appendix D2*: Access to Occupational Health Records Posting*
Appendix D3: *Global Harmonization Addendum*
Appendix D4: *Pictograms*

Effective: July 1, 2022

James H. Gailey
County Manager

#14: Credit Card Policy

I. PURPOSE

The purpose of this policy is to outline the requirements for the proper use of County credit cards. The use of credit cards has become a necessary charge vehicle for more efficient purchasing, as well as the standard requirement for most travel accommodations. While the County recognizes the need for credit cards, they must be utilized in a prudent and professional financial manner. The outline below clearly defines the expectations whenever the use of a credit card is warranted by a County employee.

II. AUTHORIZATION

The County Manager, or County Commissioners, are the only entities that can authorize the issuance of a new credit card to a County employee or department head.

III. RESTRICTED USE

The use of a County credit card is subject to the following restrictions:

A. No personal or private expenditure shall be charged to a County account.

B. No regular operating expenses (i.e., monthly telephone charges, etc.) shall be charged to a credit card.

C. Each expense charge must be accompanied by a receipt and a brief explanation. (For example, if the expense is for meals or food, note on the receipt if it was for a luncheon meeting and how many by name were included on the bill.) In other words, each expense should have the same type of documentation that you would include on a request for reimbursement.

D. Travel expenses (i.e., airfare, hotel room, conference registrations)

E. Clear documentation and receipts shall be submitted and attached to each credit card statement prior to payment. One receipt should be attached reflecting each charge on the card. If no receipt is available, then a note with full explanation shall accompany the statement.

F. No cash advances will be permitted on the County credit card.

G. All statements shall be submitted with required documentation in a timely manner to the Finance Department. No late fees or interest payments should be incurred as a result. Expenses without proper documentation shall be the responsibility of the cardholder (employee).

IV. VIOLATIONS

Violations of the County's credit card policy shall result in disciplinary action, including termination of employment and/or prosecution.

EFFECTIVE: March 11, 2019

#15: CJIS Security

I. PURPOSE

The purpose of this Administrative Regulation is to ensure the security and integrity of the CJIS network and information in accordance with CJIS and METRO policies.

II. DEFINITIONS

AIU – Access Integrity Unit, division of the Maine State Police which provides access, support and training of the METRO, NLETS, and NCIC systems.

CJIS – Criminal Justice Information Services, division of the FBI which provides access to NIC and other nationwide criminal justice information.

LASO – Local Area Security Officer, security liaison with the Maine State Police, CJIS Systems Agency and Information Security Officer.

METRO – ME Telecommunications and Routing Operations system, State network which facilitates the exchange of criminal justice information and messages.

TAC – Terminal Agency Contact, information access liaison with the AIU.

III. POLICY

All personnel with access to CJIS information provided through the County of Cumberland, hereafter referred to as "the County", will abide by the policies and procedures set forth in the Maine METRO manual and the CJIS Security Policy.

A. CJIS Information

CJIS Information may be viewed only by authorized personnel and used only for official criminal justice purposes.

B. Physical Security

1. All computers and related infrastructure with access to CJIS information must have adequate physical security so as to prevent unauthorized access to CJIS information. Outside agencies that access CJIS information through the County will be responsible for maintaining physical security at their location consistent with this policy.

2. Personnel who have not undergone a fingerprint based background check must be escorted at all times when in a CJIS secure area.

C. Personnel Security

1. All personnel will be identified by a unique user name to be used when accessing the CJIS network.

2. All personnel with access to CJIS information will undergo a fingerprint based background check within thirty (30) days of employment. Outside agencies that

access CJIS information through the County will be responsible for performing fingerprint based background checks on their employees and providing this information to the County.

3. Upon separation of employment, Human Resources or the appropriate agency official will notify the County's Information Technology Department, who will disable the employee's user account.

D. Technical Security

1. All computers and network devices with access to the CJIS network must meet the following requirements:
    a) Protected with up to date antivirus software (computers only)
    b) Operating system patches kept up to date
    c) Unnecessary services and applications disabled
    d) Unused user accounts disabled
    e) Default passwords changed

2. CJIS information transmitted electronically outside the secure network will be encrypted using a minimum 128-bit encryption algorithm.

3. The IT department will be responsible for maintaining a network map of all devices connected to the CJIS network through the County, The LASO or TAC for outside agencies that access CJIS information through the County will be responsible for providing the County with updates when changes occur on their network.

E. Remote User Access

1. Successful and unsuccessful authentications will be logged and stored in a secure location for a minimum of ninety (90) days.

2. All CJIS information transmitted to a remote location will be encrypted using a minimum 128-bit encryption algorithm.

3. Remote access from non-secure locations shall require advanced authentication in accordance with the CJIS security policy.

4. Mobile devices, such as cell phones, tablets, and mobile data computers, must be secured with a unique password or PIN. The password or PIN should be as secure and complex as allowed by the device.

F. Remote Agency Access

1. Criminal Justice Agencies served by the County's Regional Communication Center may access the CJIS network through the County's network.

2. Any criminal justice agency accessing the CJIS network through the County's network must sign the County's CJIS Service Level Agreement and abide by the County's CJIS policy.

3. Violations of County Policy, State or Federal law may result in the criminal justice agency being denied access to the County's network.

G. Passwords

1. Passwords used to access CJIS information, including access directly to the CJIS network and access to hardware or software in which CJIS information is stored will be subject to the following requirements:

   a) Passwords shall contain a minimum of eight (8) characters
   b) Passwords shall not be a dictionary word or proper name
   c) Passwords shall not be the same as the user name
   d) Passwords shall be changed every ninety (90) days
   e) The system shall prevent reuse of the last ten (10) passwords
   f) Passwords shall not be transmitted in clear text outside the secure network

H. Media

1. All media, including hard drives, USB drives, CDs and paper, which contain CJIS information, must be securely destroyed in accordance with CJIS policy prior to disposal to preclude unauthorized viewing.

2. Any electronic media used to store CJIS information that is to be reused for non-CJIS information will be turned over to the IT department to be sanitized prior to being reused.

I. Training

All employees who manage or have access to CJIS information or the hardware or software on which CJIS information is stored will receive every three (3) years thereafter. Documentation of current security awareness training for all required employees will be kept on file by the LASO for review.

J. Incident Response

1. Any suspected breach security relating to CJIS information or the CJIS network will be immediately reported to the Information Technology Department.

2. Upon being notified of a potential incident, the Information Technology Department will immediately investigate and attempt to determine the validity and scope of the incident.
3. Any confirmed security incident will be reported to the AIU in accordance with the METRO policy.

K. Discipline

Any employee found to have violated the policies of the County, Maine State Police or Criminal Justice Information Services may be subject to discipline as outlined in Cumberland County Administrative Regulation 22 as well as applicable State and Federal laws.

#16: Accepting Grants and Other Funding Resources

I. PURPOSE

The purpose of this policy is to set forth an overall framework for guiding the County's use and management of grant submissions and resources.

II. GENERAL POLICY

Grant revenues are an important part of the County's overall resource picture, especially in funding capital improvements. Although grant programs themselves are being reduced, becoming more competitive and requiring more post-award data and paperwork, actively seeking out grant revenues that assist in achieving identified County goals and objectives play a key role in the County's overall financial health strategies.

The purpose of this policy is to ensure that each grant application submitted by or on behalf of the County is aligned with an established County priority, meets the County's expectations of document quality, has matching funds available if required by grantor, and that the means for continuation of the project or program after the grant period ends has been given realistic consideration.

III. GRANT OVERSIGHT COMMITTEE

A Grant Oversight Committee shall be established to review and provide guidance and approvals on all grant applications (new/renewal) submitted by County Departments. All grants prior to submission shall be processed through the Oversight Committee. This Committee shall include:

A. A County Commissioner,

B. County Manager,

C. County Treasurer

D. Audit and Compliance Manager.

IV. PROVISIONS

GOALS

A. To set forth the importance of grant programs in accomplishing County goals and objectives.

B. Establish general concepts and framework for seeking and managing grant programs.

C. Identify roles and responsibilities in managing grant programs.

D. Establish criteria for evaluating the benefits and costs of grant programs.

E. To set forth the County's policy in complying with Single Audit Act requirements.

V. GENERAL CONCEPTS AND FRAMEWORK

A. The County will aggressively pursue grant funding from federal, state and other sources, consistent with identified County goals and objectives.

B. Aside from entitlement grants, the County shall focus its efforts on securing grants for capital improvements. This approach will allow the County to compete for projects we might not otherwise be able to afford while maintaining financial independence should future grant sources diminish.

C. Grants for operating purposes may be considered on a case-by-case basis after careful consideration of the benefits of the program and the ongoing impacts on the County if grant funding is no longer available.

D. For "Pilot Programs" The County shall go through a significant review and conversation with the County Commissioners of whether to apply for grants that fund "pilot" operating programs or short-term staffing enhancements to existing programs. Taking on these programs could ultimately aggravate the County's fiscal position should the desire for the program remain once the grant funding is no longer available.

E. The County will only seek grants when sufficient staff resources are available to effectively administer the program in compliance with grant requirements and successfully perform the grant workscope.

F. Indirect costs of administering grant programs will be recovered to the maximum extent feasible.

G. Departments have the primary responsibility for seeking out grant opportunities, for preparing effective grant applications and for successfully managing grant programs after they have been awarded.

H. Departments should develop a simple system that tracks grant funding availability in their functional areas. Using this system, all capital improvement plan budget requests will evaluate and document the ability of grants to assist in funding the project.

VI. ROLES AND RESPONSIBILITIES

A. County Commissioners

1. Approves grant management policies.
2. Approves all grant applications which require additional County resources, obligations (matching funds) and short/long-term tax rate impact that are not budgeted and delegates receipt and contract execution to the County Manager if delegation is allowed by the grantor agency.
3. Approves all grant awards for all county departments whether capital or programmatic focused.
4. Seeks guidance from Grant Oversight Committee and in unique circumstances relies on the Committee to act on the Commissioners behalf.

B. County Manager

1. Is the point person for all grants requesting to be submitted on behalf of the County. Depending upon the type and intent of the grant, County Manger shall determine what process the grant approval process shall take.

2. Receives grants and executes related contract documents when delegated to do so by the Commissioners.

3. Works with Department to appropriate funding when applicable.

4. Develops, recommends and maintains grant management policies.

C. County Treasurer

1. The County Treasurer, is responsible for the oversight of the County's financial activity. In this role, Finance has the authority to review financial reports generated by recipient departments, work with the County Attorney to identify and investigate issues that may arise with respect to the management of County grants, and provides general oversight of other grant financial related issues, including the proper budgeting and accounting for grants and other responsibilities indicated throughout this policy.

2. The County Treasurer oversees/approves the pre-submission and post-award of the grant.

3. Finance is responsible for creating a grant fund and/or project number, which is used to recognize grant revenue and expenditures in the department or division's budget.

4. Coordinates preparation and distribution of single audit reports. Ensure that the County's policy regarding single audit act requirements is implemented.

D. Departments (Directors/Project Managers)

The Director shall designate a Project Manager designated for all grant oversight and responsibility. This Project Manager shall be responsible for handling all grant administration as it relates to reporting and documentation in relevant granting agencies and shall:.

1. Develop systems for maintaining ongoing information regarding grant availability within their functional areas of responsibility.

2. Evaluate benefits and costs of specific grant programs on a case-by-case basis:

    a. Purpose of the grant program and its consistency with identified County goals and objectives.

    b. Additional staffing, office space, facilities, supplies or equipment that will be required if the grant is awarded.

    c. Develop a report on the ongoing impacts of the grant program after it is completed.

    d. Responsibilities of other departments and impacts on them in preparing the grant application or performing work scope if the grant is approved.

e. Amount of indirect costs to be recovered from the grant,

f. Total program costs, including portion funded through grant revenues and any required County contribution.

g. Source of funding for any required County share.

h. Compliance and audit requirements, paying special attention to those areas where the grantor's administrative procedures are different than the County's.

3. Prepare grant applications.

a. All proposed grants shall be submitted to the Grant Oversight Committee for review and guidance based on conditions that are voted on by the Oversight Committee annually. Once the department determines they will be applying for the grant, the **Grant Authorization Form** shall be submitted to the Oversight Committee. For grants approved by the Committee and require additional unbudgeted County resources, those grants shall seek County Commissioner approval prior to submission.

b. Work with the grantor agency in identifying special program requirements and developing strategies for preparing a successful grant application.

c. Complete grant application documents.

d. Coordinate with affected departments as necessary.

4. Administer grant programs if awarded.

a. Notify County Manager & County Treasurer of the award.

b. Prepare a Staff Report requesting the accepting grant award, including grant summary form, budget amendment request and any other required County forms or documents; and coordinate execution of grant documents by the County Manager and return executed documents to grantor agency.

c. Notify affected departments of grant award.

d. Maintain financial and other records in accordance with grant requirements.

e. Complete and submit required reports, including requests for funds.

f. Monitor grant expenditures and receipt of revenues.

g. Coordinate on-site management reviews by the grantor agency during the grant term.

h. Ensure compliance with grant requirements, paying special attention to those areas where the grantor's administrative procedures are different than the County's.

i. Perform the grant work scope.

j. Project Managers will reconcile proposed reimbursement requests with the appropriate General Ledger information prior to submitting reimbursement requests.

5. Complete grant closeout.

a. Complete the grant work scope.

b. Notify affected departments that the project is completed and schedule a "close-out" meeting if necessary to resolve any final procedural issues.

c. Ensure final receipt of grant revenues.

d. Prepare and submit any required grant close-out documents.

e. Review grant file for completeness.

f. Retain all necessary program and financial records for the period of time required by grantor agency.

g. Coordinate any on-site management reviews or audits after the grant is completed.

h. Resolve any audit findings.

VII. CONFLICT OF INTEREST

Grant audit findings due to conflicts of interest can damage the reputation and credibility of the County. Further, the appearance of a conflict of interest can be just as damaging to the County's reputation and credibility as an actual conflict. The purpose of this policy is to avoid the appearance, as well as the actuality, of any conflict of interest or breach of trust by an official or employee of the County.

A. No officer or employee of the County shall have any interest, financial or otherwise, direct or indirect, or have any arrangement concerning prospective employment that will, or may be reasonably expected to, bias the design, conduct, or reporting of a grant funded project on which he or she is working.

B. The Department Director and/or Project Manager for each particular grant funded project shall ensure that in the use of project funds, officials or employees of the County and nongovernmental recipients or sub-recipients shall avoid any action that might result in, or create the appearance of:

1. Using his or her official position for private gain

2. Giving preferential treatment to any person or organization
3. Losing complete independence or impartiality
4. Making an official decision outside official channels
5. Affecting adversely public confidence in the grant funded program in particular and the County in general
6. Any violation of this provision is governed by any County's Policies & Procedures.

VIII. INTERNALLY COMPETING APPLICATIONS

Grantors generally will not consider any proposal from a jurisdiction if that jurisdiction has submitted more than one proposal during the same funding round. Even if the grantor allows competing applications from the County, it may not be in the best interest of the County to compete against itself. The purpose of this policy is to identify the procedure for resolving such conflicts.

IX. AUTHORIZED WRITTEN SIGNATURE

The purpose of this policy is to identify who may approve and provide authorized written signatures on grant applications and subsequent grant agreements. This shall be done well in advance of grantsubmission due dates to avoid last minute delays or problems that could cause the grant deadline to bemissed.

A. This written signature authority is different from the electronic signature authority granted to specific individuals in departments for the purposes of submitting an online grant application or quarterly reports as indicated in Section below.

B. There are three authorized grant application signers: County Manager, County Treasurer and Department Directors.

C. Authority over a specific grant project or program, grant application or grant agreement may be delegated in writing to address circumstances that warrant delegation to a or provide efficiency.

D. If a grantor requests a signature other than what is defined above, a copy of this policy may be provided to grantors as documentation authorizing that person to sign.

X. AUTHORIZED ELECTRONIC SIGNATURE PROCEDURE

Many federal and state grant programs have the requirement or option of submitting grant applications and reporting through the internet. The purpose of this policy is to identify the procedure to provide authorized electronic signatures.

A. All grant applications submitted through the internet shall comply with the standard policies and procedures for submission of grant applications as described in this policy.

B. The individual submitting the grant must be designated as an authorized electronic signatory by his/her Department Director.

C. The Department Director shall send an email to the County Treasurer notifying authorized electronic signature status for each designated staff person he/she selects. This shall be done well in advance of grant submission due dates to avoid last minute delays or problems that could cause the grant deadline to be missed.

XI. AWARD NOTIFICATION AND ACCEPTANCE

Grant agreements are legal contracts. It is the County's responsibility to carry out the project and/or activities associated with a grant to accomplish its objectives, while adhering to all of the terms and conditions prescribed by the grantor. Failure to do so increases the County's exposure to legal liability and compromises current and future grant funding. Therefore, the County carries a significant legal and ethical responsibility when accepting grant funding.

The award notification, review and acceptance process have two components: (1) award notification and (2) County Commissioners approval to accept the award.

A. Award Notification Procedure

All departments that receive a grant award shall date stamp, duplicate, and forward a copy of the award notification, the grant agreement or contract, and any memoranda of understanding to the County Treasurer within one week of receipt.

B. Comm**issioners Approval To Accept Award Procedure**

The purpose of this policy is to ensure that acceptance of each award granted to the County is formally authorized by County Commissioners no matter what size, duration or intent.

1. If approval of the Grant has not been previously authorized by the County Commissioners, the County Commissioners shall review the item for consistency to this policy and may deny receipt of said grant if the grant has a budgetary impact. The County Commissioners may ask the County Manager to prepare a Commissioners Agenda Staff Report outlining and fiscal impact statement requesting County Commissioners authorization for the County Manager to execute the Grant Agreement and related documents.

2. Once executed by the proper County Officials, the Project Manager will forward the executed document to the Grantor.

3. The fully executed original Grant Agreement (executed by the County and the Grantor) shall be received by the appropriate Department and a copy sent to the Finance Department.

XII. GRANT REPORTING

Grants awarded to the County may require that progress, programmatic and financial reports be submitted to the grantor. Accurate and timely reporting is critical to maintaining a good relationship with the grantor. Late or inaccurate reports may negatively impact current or future funding.

XIII. GRANT REPORTING PROCEDURE

A. Recipient departments must prepare timely and accurate progress, programmatic or financial reports as required by grantor.

B. Copies of all financial status and final reports prepared for submission to the grantor shall be provided, along with the associated grant name and year to the County Treasurer or his/her designee at the time of submission to the grantor.

C. The County Treasurer or his/her designee will review the financial reports for content and quality and address any issues with the recipient department to better assist for future reports.

XIV. GRANT FILE MANAGEMENT, ACCESS AND RETENTION

The County Manager, County Treasurer/Finance Director may review the files, activities, equipment, and facilities, and interview relevant personnel and contracted entities of any County project or program that is funded with grants awarded to the County.

A. FILE MANAGEMENT PROCEDURE

All department and master files associated with a grant award must maintain a file structure that includes the following five sections with clear separations between different fiscal years, unless otherwise directed by the grantor:

1. **Submittal** (e.g., application guidance and a copy of the application)
2. **Research** (e.g., statistical and other information used in preparation of and support of the grant)
3. **Award** (e.g., award letter, Commissioners agenda item, grant agreement, grant amendments, modifications, extensions, cancellations and terminations and anything else related to the award)
4. **Finance** (e.g... account set up. purchase orders, invoices)
5. **Reports** (e.g., reports to granting entity and evaluation components)

B. FILE RETENTION PROCEDURE

The County maintains records in accordance of the Maine State Archives Administrative Schedule 1.14 Grants for at least three years following the closure of its most recent audit report. If any litigation, claim, negotiation, audit, or other action involving grant records has been started before the expiration of the three-

year period, the records must be retained until completion of the action and resolution of all issues which arise from it, or until the end of the regular five-year period, whichever is later.

1. Grantors may require retention periods in excess of five years. Departments must ensure they comply with retention requirements specified by each grantor.

2. Retention requirements extend to books of original entry, source documents supporting accounting transactions, the general ledger, subsidiary ledgers, personnel and payroll records, cancelled checks, and related documents and records.

3. Source documents include copies of all awards, applications, and required recipient financial and narrative reports. Personnel and payroll records shall include the time and attendance reports, personal activity reports or equivalent documentation for all individuals reimbursed under the award.

XV. GRANT CLOSEOUT

Upon completion of the grant term of each grant award, the recipient department shall alert the County Treasurer to place the fund and/or project in a no posting status.

A. PROCEDURE

Upon completion of the grant period of each grant, the recipient department must prepare a memorandum to the County Treasurer that identifies the name of the grant, the project number and describes the final disposition of the funds and required activities.

XVI. SINGLE AUDIT ACT REQUIREMENTS

The County is subject to the financial and compliance requirements of the Single Audit Act of 1984, which is applicable to all local and state governments expending more than $750,000 in federal financial assistance during a fiscal year. The purpose of the Act is to:

A. Improve the financial management and accountability of state and local governments with respect to federal financial assistance programs.

B. Establish uniform requirements for audits of federal grants.

C. Promote efficient and effective use of audit resources.

D. Assure that federal departments and agencies rely upon and use audit work performed during a single audit rather than performing the audit work themselves.

E. Under this Act, federal grants are included under an inclusive single audit program that is incorporated into the County's annual audit and financial report preparation process. During the audit, tests are made to determine the adequacy

of the internal control structure, including that portion related to federal financial assistance programs, as well as to determine that the County has complied with applicable laws and regulations

XVII. POLICY REGARDING SINGLE AUDIT APPROACH

For federal grants included in the scope of the County's single audit approach, it is the County's policy that all financial and compliance issues have been met through the single audit, and follow-up audits to determine these issues are not necessary unless specifically related to findings or recommendations included in the single audit report. As noted above, the purpose of the Act is to establish uniform audit requirements, promote efficient use of audit resources, and assure that federal agencies rely upon audit work already completed; its purpose is ***not*** to audit local agencies twice. Accordingly, the County will strongly resist any efforts by federal agencies to duplicate audit work already performed in complying with Act requirements. As such, whenever federal grantor agencies request final audits, the managing department should notify the Finance Department in order to ensure a consistent response to these types of requests.

XVIII. ATTACHMENTS

Appendix G1 *Grant Authorization Form*

EFFECTIVE: DECEMBER 12, 2022

#17. Temporary Telework Policy

In exceptional situations including cases of public emergency and/or in compliance with public health guidance for contagious diseases, Temporary Telework may be approved for temporary alternative work arrangements. This is a short-term discretionary program and must be discussed and considered on a case-by-case basis with the department head and/or division supervisor and individual employee(s).

This policy does not apply to employees who are considered "essential" during those times of emergency or public health issue.

Any employee who works off-site must use reasonable caution, procedures and equipment that maintains data storage and transmission security.

For purposes of Temporary Telework, the General Provisions below shall apply. The employee and/or job classification (preferred) shall be pre-qualified through a review by their department head and the Human Resources Director to Telework, a copy of which shall be stored in the employee file and/or within a file in the department. Emergency Management will send out questionnaire annually with a due date of July 1st.

I. GENERAL PROVISIONS

A. Communication.

While teleworking, the employee shall be reachable by either phone, text, fax, or e-mail during agreed-upon work hours. The employee and supervisor shall agree on expected turnaround time for responses.

B. Conditions of Employment.

The teleworker's conditions of employment shall remain the same as for non-teleworking employees; wages, benefits and leave accrual will remain unchanged.

C. Equipment.

Home worksite furniture and computer equipment shall generally be provided by the teleworker. In the event that equipment and software is provided by the County at the telework-site, such equipment and software shall be used exclusively by the teleworker and for the purposes of conducting County business. If the County provides equipment, the teleworker is responsible for safe transportation and set-up of such equipment.

D. Equipment liability.

The County will repair and maintain, at the primary worksite (designed County building), any equipment loaned by the County. Surge protectors must be used with any County computer/printer made available to the teleworker. The employee will be responsible for:

- any intentional damage to the equipment;
- damage resulting from gross negligence by the employee or any member or guest of the employee's household;
- damage resulting from a power surge if no surge protector is used;

The County may pursue recovery from the teleworker for County property that is deliberately, or through negligence, damaged, destroyed, or lost while in the teleworker's care, custody or control. Damage or theft of County equipment that occurs outside the employee's control will be covered by the County. Teleworkers should check their homeowner's/renter's insurance policy for incidental office coverage. The County does not assume liability for loss, damage, or wear of employee-owned equipment.

E. Dependent Care.

Telework is not a substitute for childcare or other dependent care. Teleworkers shall make or maintain childcare arrangements to permit concentration on work assignments.

F. Home Work Site.

The teleworker must establish and maintain a dedicated workspace that is quiet, clean, ergonomically appropriate and safe, with adequate lighting and ventilation. The teleworker will not hold business visits or meetings with professional colleagues, customers, or the public at the home worksite. Meetings with other County staff will not be permitted unless approved in advance by the employee's supervisor.

G. Hours of Work.

The teleworker will have regularly scheduled work hours agreed upon with the supervisor, including specific core hours and telephone accessibility. Overtime work for a non-exempt employee must be pre-approved by the supervisor. The teleworker will attend job-related meetings, training sessions and conferences, as requested by supervisors. In addition, the teleworker may be requested to attend "short-notice" meetings. The supervisor may use telephone conference calling whenever possible as an alternative to requesting attendance at "short-notice" meetings.

H. Incidental Costs.

Unless otherwise stated in the Telework Agreement, all incidental costs, such as residential utility costs or cleaning services, are the responsibility of the teleworker.

I. Inclement Weather.
If the temporary worksite is impacted due to an emergency or power outage, the teleworker will notify the supervisor as soon as possible. The teleworker may be reassigned to an alternate worksite or depending upon the situation be unable to telework. The department head/supervisor will make the determination.

J. Inspections.
In case of injury or occupational illnesses, theft, loss, or tort liability related to telework, the teleworker must allow agents of the County to investigate and/or inspect the telework site.

K. Injuries.
The employee will be covered by workers' compensation for job related injuries that occur in the designated workspace, including the teleworker's home, during the defined work period. In the case of injury occurring during the defined work period, the employee shall immediately report the injury or occupational illnesses to the supervisor. Workers' compensation will not apply to non-job related injuries that might occur in the home. The County does not assume responsibility for injury or occupational illnesses to any persons other than the teleworker at the telework-site.

L. Intellectual Property.
Products, documents, and records developed while teleworking are property of the County.

M. Leave.
The telework employee must obtain supervisory approval before taking leave in accordance with County policy.

N. Network Access.
The County is committed to supporting telework by allowing network access from remote locations. However, network access is not guaranteed.

O. Office Supplies.
The County shall provide any necessary office supplies. Out-of-pocket expenses, approved by the employee's supervisor, for supplies normally available in the office will be reimbursed.

P. Performance & Evaluations. The supervisor and teleworker will formulate objectives, expected results, and evaluation procedures for work completed while the employee is teleworking. The supervisor will monitor and evaluate performance by relying more heavily on work results rather than direct observation. The supervisor and telework employee will meet at regular intervals to review the employee's work performance.

Q. Personal Business.

Telework employees shall not perform personal business during agreed upon work hours.

R. Policies.

County policies, rules and practices shall apply at the telework site, including those governing communicating internally and with the public, employee rights and responsibilities, facilities and equipment management, financial management, information resource management, purchasing of property and services, and safety. Failure to follow policy, rules and procedures may result in termination of the telework arrangement and/or disciplinary action.

S. Quality of Work

All work shall be performed according to the same high standards as would normally be expected at the primary worksite.

T. Record Retention.

Products, documents and records that are used, developed, or revised while teleworking shall comply with Administrative Regulation #8 and be stored to the County's server.

U. Security.

Security and confidentiality shall be maintained by the teleworker at the same level as expected at all worksites and in compliance with Administrative Regulation #15.

V. Taxes.

A home office is not an automatic tax deduction. Teleworkers should consult with a tax expert to examine the tax implications of a temporary home office.

W. Telephone/Internet Expenses.

The teleworker and supervisor will use the most efficient and effective way of handling telephone and internet use fees.

X. Travel.

Time and mileage will be paid in accordance with FLSA regulations.

#18. Emergency Essential vs Non-Essential

A. Emergency and Non-Emergency Employees

Emergency employees are employees who are expected to report to their worksite or begin teleworking (as permitted) on time unless otherwise directed by their department heads/supervisors. The County advises departments to designate in advance those emergency job classifications critical to agency operations (including security and infrastructure) in dismissal or closure situations and who will be expected to work. The County does not provide standard Government wide definitions of emergency employees due to the diversity in agency missions and employee occupations/skills, the variable nature of the emergencies, and weather and geographic conditions specific to duty locations.

Each department is in the best position to determine its own needs and is responsible for determining which employees are designated as emergency employees. Department heads (or their designees, as applicable) should make such determinations based on the department's unique mission requirements and/or circumstances and seek approval from the County Manager and Human Resource Director prior to the July 1st annual deadline. Such designations should be communicated to the affected employees at least annually (preferably in writing and well in advance) so employees can be prepared to support and sustain County operations.

Those non-emergency employees who are not required to report to work or telework, will be reviewed and based on longevity of emergency and the County's financial position, the County Manager and Commissioners will make a determination on whether the time is paid or unpaid. If unpaid, employees will be allowed to use available benefit time to the extent it is available.

When Government operations are disrupted and offices are closed for an extended period of time, the County Administration may determine that changing circumstances require non-emergency employees to report for work. Consequently, each department should establish a procedure for notifying and recalling these employees. THE COUNTY advises departments to identify non-emergency employees who are expected to remain in contact with their departments at all times during dismissal or closure situations to maintain continuity readiness. Such employees may be called to work during emergencies dealing with national security, extended emergencies, or other unique situations. Employees may be directed to aid another department, who during the emergency may need additional staff capacity to perform their tasks. A department should anticipate the emergency situations in which such employees will be expected to report for work at a regular worksite or alternative worksite and the circumstances under which employees will be permitted to telework, if the agency prefers, and should notify affected employees of this policy.

B. Interaction of Weather and Safety Leave and Emergency Employees

Emergency employees are expected to report to or remain at their worksite unless otherwise directed by their department head. Generally, emergency employees do not receive weather and safety leave. During certain emergencies, the County Administration may determine that the circumstances have made traveling to or performing work at the worksite unsafe for emergency employees. In these situations, a particular department may either require the emergency employee to work at another location or determine that circumstances justify providing weather and safety leave to emergency employees.

If an employee who is required to work fails to report for work without adequate reason for his or her absence, the department may place the employee on absence without leave, and the employee may potentially be disciplined by the department head. Each department, in conjunction with the Human Resources Department, is responsible for determining whether the employee has adequate reasons for his or her absence.

C. Employees on Preapproved Leave (Paid or Unpaid) or Other Paid Time Off

THE COUNTY's weather and safety leave regulations do not allow employees to receive weather and safety leave for hours during which those employees are on preapproved leave or other paid time off. Periods of paid leave include earn time, vacation, personal days, holiday and sick leave. Agencies should not approve weather and safety leave for an employee, who in the department's judgment, requests to cancel his or her preapproved leave (paid or unpaid) or paid time off primarily for the purpose of obtaining weather and safety leave. If the employee was not expected to report to duty during a period for which weather and safety leave might otherwise have been authorized, there is generally no need for the agency to provide weather and safety leave to relieve the employee from his or her obligated workday (e.g., work hours). Supervisors may request sufficient information or documentation to show that granting weather and safety leave is appropriate—for example, documentation that the same weather/safety event caused cancellation of travel plans or of a doctor appointment.

#19 Cumberland County Emergency Pay Policy

I. POLICY:

It is the policy of Cumberland County to set up special compensation provisions for employees who work during an "emergency." "Emergency" shall include, but not be limited to, man-made disasters, act of terrorism and natural disasters such as hurricanes, floods, storms, etc. It is also the policy of Cumberland County to outline the responsibilities of its employees during and after the existence of an emergency.

Until the County can determine the extent of the "Emergency", all employees of Cumberland County should plan they are working before, during, or after an Emergency. All employees are required to call their Supervisor, Department Director, or reference the County's website in order to receive instructions on whether they are working, if so, where and when to report. Employees who fail to contact one of the above during an emergency will be subject to immediate disciplinary action up to and including termination, unless an employee can prove that lack of phone and internet service prevented them from calling.

II. PROCEDURE:

A. Full time and part time employees designated as Emergency Essential will be required to be available to work either before, during or immediately after an emergency occurs. Exactly when and where an employee shall be required to work will be determined by either their Department Director or the County Manager or designee. All non-exempt employees who are required to work shall be paid their regular rate of pay for all hours worked unless those hours result in overtime, in which case payment will be at time and one half for all hours worked above 40 hours per week, or in accordance with collective bargaining agreements.

    1. If an employee and their spouse both work for the County, they may both be required to work; however, the County may allow them to work different shifts if requested. This also applies to employees whose spouse works for the Sheriff's Department or another first responding agency, as determined by Human Resources and the Department.

B. In the case of any government closings that result from an emergency, all employees will be required to contact either their Supervisor or Department Director in order to find out if, when and where they will be working. All Emergency Essential employees, regardless of current position, will be expected to work either immediately before, during, or immediately after an emergency. Employees may be required to perform their normal duties before, during or after the emergency; or they may be required to perform work specific to an emergency event.

C.

1. All employees will be given a time and a location where they are to report in the event of an emergency. This information will either be distributed prior to an event if time allows, or may be conveyed to employees after they call their supervisor, department director or refer to the County's website if available. Full-time and part-time employees will be notified to the extent they are needed during the emergency event.

2. Non-Emergency employees may be required to work flexible hours. Working a flexible schedule may be necessary in order to accommodate the needs of the County during the Emergency. All hours worked will be paid at regular time unless overtime applies for hours over 40, or in accordance with collective bargaining agreements.

D. The County Manager may at any time during an emergency, make a declaration "Suspending All Government Operations". The County Manager or his/her designee may "suspend all government operations" when conditions are such that no work is able to be performed due to the nature of the emergency. Emergency response personnel is defined as Sheriff's Office, Jail, Regional Communications, Emergency Management and in some instances Facilities, Finance and Human Resources. Employees within these departments are expected to report to work, unless otherwise notified differently.

E. Under certain emergency or disaster conditions, Exempt Employees may be required to work extended hours due to the nature of the emergency. Exempt employees may be authorized for additional payment in such situations. The duration as well as the circumstances under which such payment will be made, will be at the discretion of the County Manager with concurrence of the County Commissioners, under the following guidelines:

1. The County Manager shall determine, on a case by case basis, whether exempt employees are to be reimbursed for additional hours worked during an Emergency. As part of the County Manager's deliberation, he or she shall include such factors as the hours spent working on the event, the extent of damage incurred in Cumberland County from the event, whether or not the event occurred mainly during normal business hours, and other extenuating circumstances that may come to his or her attention.

#20 Regional Aid Fund

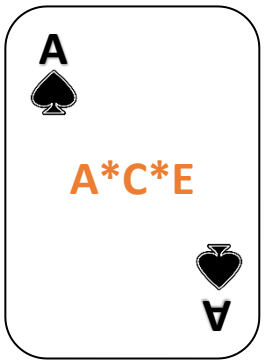
I. PURPOSE:

The County shall establish a Regional Aid Fund to set-a-side financial resources that may be used to aid in a regional crisis. Regional crisis, includes, but is not limited to the following: homelessness, food insecurity, clothing, transportation, transitional living arrangements and services associated with breaking down language or cultural barriers. The following guidelines shall be followed in the administration of this Fund:

A. Any funds transferred into the reserve account is only by vote of the County Commissioners;

B. Expenditure of funds of up to $1,000 can be made by the County Manager in consultation with the Board Chairman, up to three times a year. Expenditures in excess of $1,000 shall seek authorization from the County Commissioners.

C. Subject to the annual review of the County Commissioners Contingency Account, a determination shall be made on whether the overall budget has suitable funding to make a year-end balance transfer from the Commissioner Contingency account to the Regional Aid Reserve Account. The Reserve Account shall be capped at $75,000.



Appendix A1 – Nomination Form

*A*C*E (Acts of Commitment and Excellence) Nomination Form*

Cumberland County wants to recognize employees who demonstrate acts of commitment and excellence and you can help us find them! When you see or hear about someone who you think deserves to be recognized, please fill out this nomination form.

Please include job description for nominee with this form (contact Human Resources for copy if needed). If necessary, use the reverse of this form or additional pages.

I would like to nominate:

Department he/she works in:

Hired date: (applicants are not eligible unless they've completed one (1) consecutive year of service)

Based on: ☐ Sustained performance

☐ Single act on

1. Explain how the employee's actions substantially exceeded the expected job performance over a sustained period of time (if applicable).

2. Explain the employee's work on a specific project or single act that resulted in significant cost savings or a highly desirable benefit to operations.

Nominator		Phone #/extension	
Nominator Signature:			
Supervisor Signature:			

Appendix B1 – Management Roles and Responsibilities

CUMBERLAND COUNTY SHERIFF'S OFFICE

Standard Operating Procedure

Title: Schedule of Fees	**No.: A-39**
Effective Date: 6-7-2017	**Distribution: All Personnel**
Review Date: 6-1-2018	**Number of Pages: 2**
Rescinds: Policy 2-31A, dated 8-1-2012	**Accreditation Standard: N/A**
Associated With: N/A	**Sheriff's Signature: *Kevin J. Joyce*** ***Electronic Signature/ Approval 6/6/2017***

I. **POLICY:** It is the policy of the Cumberland County Sheriff's Office to provide a fee structure for those services that cover the Freedom of Access Act (FOAA) and other requests for the law enforcement and jail divisions of this agency.

II. **PURPOSE:** It is the purpose of the Cumberland County Sheriff's Office to provide a fee structure for a wide range of police services to the community we serve. Frequent services often requested include;

A. Requests for copies of reports and alternate media forms.

B. Civil Division same day service.

C. Pre-employment polygraphs.

D. Fingerprinting.

III. **FEES:**

A. **Requests for copies of reports or alternate media forms:**

1. Report (FOAA/Accident) $0.10 per page
2. Color photos on printed paper: $2.00 each
3. Non-paper Requests (VHS, DVD, CD, Audio): $6.00 for each request
4. Research Fee (for searching, retrieving, and compiling records): $25/hour after

first two hours free.

5. Expedited Service: $25.00
6. Conversion Charge (converting to usable format): Actual cost
7. Postage Fee: Actual cost

Note: Pre-payment must accompany request(s), unless other satisfactory arrangements have been agreed upon with the records clerk.

B. Civil Division same day service:

1. Same day service: $25.00*.

*Note: *All other fees are governed by statute or IRS.*

Pre-payment must accompany request(s), unless other satisfactory arrangements have been agreed upon with the administrative civil deputy.

C. Pre-Employment Polygraphs: This service is offered to outside Law Enforcement Agencies who can request the services of the County Polygraphist (if available), or copy of a polygraph that has already been completed.

1. The requesting agency must submit a written request.
2. In the case of a request for a copy of a completed polygraph, the requesting agency must submit a release of information form from the person whose polygraph is being requested.
3. Fees associated with polygraph:
   - Pre-Employment Polygraph: In-County: $250.00 Out of County: $300.00
   - Criminal Investigation: No Charge
   - Post-Conviction Sex Offender Test: $300.00
   - Internal Investigation: Hourly rate for the Examiner
   - Copy of Completed Exams: In-County: $250.00 Out of County: $300.00
   - Quality Control: No Charge
   - TES (Test for Espionage and Sabotage) Federal: Hourly rate for the Examiner

D. Pre-Employment Psychological Examinations <u>will not</u> be released to outside agencies.

E. Exception to Fees: At the Sheriff's discretion, any Pre-Employment Examination Fee may be waived or reduced.

Note: To assure a timely response as well as payment for the polygraph records, the Executive Assistant shall forward the appropriate information to

the Finance Director for the purpose of an invoice being generated and forwarded to the requesting agency.

F. Fingerprinting: *Note: Subjects who request fingerprints must provide their own fingerprint cards. These cards are typically provided to the subject by the organization requiring the fingerprinting.*

1. The Cumberland County Sheriff's Office offers fingerprinting which is a service that is performed by those assigned to work the jail lobby desk. Fingerprinting members of the public for non-criminal matters, at their request and the acceptance, documentation and submission of fees for performing this service for the following legitimate requests;
   - **a)** Employment applications;
   - **b)** Educational program employees/teachers;
   - **c)** Stockbrokers;
   - **d)** Medical field positions (Doctors, Nurses, etc.);
   - **e)** Law Enforcement requests.
2. Fees:
   - **a)** For one fingerprint card: $15.00.
   - **b)** For any additional cards: $5.00 each
3. No Fees: This agency will not charge fees for the following fingerprint requests:
   - **a)** Adoptions
   - **b)** Child Find Program
   - **c)** Other fingerprinting requests approved by the administration.

Appendix C1 – Management Roles and Responsibilities

Assignment of Management Roles and Responsibilities for Security

Cumberland County's policies and procedures must clearly define information security responsibilities for all personnel. (PCI-DSS Requirement 12.4)

In accordance with this requirement, the following responsibilities have been established:

1. The County Manager is the final authority for the County's governance of information security policy and procedure, including:

    - Approval of all policy specific to information security
    - Approval of all actions taken in response to any suspected or real security incidents

2. The County's Chief Information Officer is responsible for overseeing all aspects of information security, including but not limited to the following:

    - Monitoring and analyzing security alerts and distributing information to appropriate information security and business unit management personnel
    - Periodic analysis, identification, and ranking of emerging security vulnerabilities
    - Review security logs and follow-up on exceptions

3. The County Security Incident Response Team is responsible for establishing, updating, documenting, and distributing security policies and procedures, and security incident response and escalation procedures (*Incident Response Plan*) to ensure timely and effective handling of all situations involving security incidents regarding any part of the System, including:

    - Roles, responsibilities, and communication
    - Coverage and responses for all critical system components
    - Notification, at a minimum, of credit card associations and acquirers
    - Strategy for business continuity post compromise
    - Reference or inclusion of incident response procedures from card associations
    - Analysis of legal requirements for reporting compromises
    - Annual testing
    - Designation of personnel to monitor for intrusion detection, intrusion prevention, and file integrity monitoring alerts on a 24/7 basis
    - Plans for periodic training
    - A process for evolving the incident response plan according to lessons learned and in response to industry developments

The membership of the County Security Incident Response Team shall be comprised of the following County personnel:

- County Manager
- Deputy County Manager
- IT Director
- Finance Director
- Manager of Human Resources
- County Compliance Coordinator
- County General Counsel

4. The County Compliance Coordinator is responsible for coordinating the following compliance-related activities:

    - Liaison with credit card associations and acquirers on matters specific to PCI compliance
    - Coordination of the annual PCI attestation process, including:
        - Distribution of County Credit Card policy to stakeholders for review
        - Collecting and compiling any policy updates for final review and approval
        - Posting and communication of policy updates to the community at large
        - Conducting and submitting the on-line attestation questionnaire
    - Alert the County Manager or daily designee of received incident reports
    - Coordination and scheduling of activities involving the County Security Incident Response Team
    - Maintaining a formal security awareness program for all employees that provides multiple methods of communicating awareness and educating employees (for example, posters, letters, meetings)

5. The Information Technology Department shall maintain daily administrative and technical operational security procedures that are consistent with the PCI-DSS. System and Application Administrators shall perform the following roles:

    - Establish and adhere to a change control policy and process for all changes to system components
    - Perform periodic system component security testing
    - Monitor and analyze security alerts and information and distribute to appropriate personnel
    - Administer user accounts and manage authentication

- Monitor and control all access to critical data, including, but not limited to, Cardholder Data
- Retain audit logs in accordance with the County's retention policy
    - Develop software applications in accordance with PCI-DSS and based on industry best practices

6. Department Heads and supervisors are responsible for ensuring that the activities under their direction adhere to these policies and that employees participate in security awareness programs:

    - Ensuring that employees have read and understand the county's information security policies, and have attended all required educational meetings regarding the same
    - Screen potential employees and their activities to minimize the risk of compromise or exploit from within the organization

7. Internal Audit (or equivalent) is responsible for executing a risk assessment process that identifies threats, vulnerabilities, and results in a formal risk assessment.

8. The General Counsel's Office will ensure that for service providers given access to Cardholder Data, provided direct access to the Cardholder Data Network, or who can affect the security of the Cardholder Data Network the following practices are observed:

    - Contracts require adherence to PCI-DSS by the service provider
    - Contracts include written acknowledgement or responsibility for the security of Cardholder Data by the service provider

Appendix C2 - Incident Response Policy

The County Security Incident Response Team shall establish, document, and distribute security incident response and escalation procedures (*Incident Response Plan*) to ensure timely and effective handling of all situations. (PCI requirement 12.5.3)

Incident Identification

Employees, contractors, business partners, or agents must be aware of their responsibilities in detecting security incidents to facilitate the incident response plan and procedures. All parties have the responsibility to assist in the incident response procedures within their particular areas of responsibility. Some examples of security incidents that an employee might recognize in their day to day activities include, but are not limited to:

- Theft, damage, or unauthorized access (e.g., papers missing from their desk, broken locks, missing log files, alert from a security guard, video evidence of a break-in or unscheduled/unauthorized physical entry, computer not in same state as employee left it in or other indication that it has been improperly accessed, etc.)

- Fraud – Inaccurate information within databases, logs, files or paper records

- Unauthorized wireless device detected on the network

Reporting an Incident

The County Compliance Coordinator should be notified immediately of any suspected or actual security incidents involving Cardholder Data:

- Contact the County Compliance Coordinator to report any suspected or actual incidents. The Internal Audit's phone number should be well known to all employees and should page someone during non-business hours.

- No one should communicate with anyone outside of their supervisor(s) or members of the County Security Incident Response Team about any details or generalities surrounding any suspected or actual incident. All communications with law enforcement or the public will be coordinated by the County Executive Office under the direction of the County Commissioners.

- Document any information you know while waiting for the County Compliance Coordinator to respond to the incident. If known, this must include date, time, and the nature of the incident. Any information you can provide will aid in responding in an appropriate manner.

- In response to a received report, the County Compliance Officer shall alert the County Manager or, if absent, the person in charge for the day. It shall then be the decision of the County Manager or daily designee to convene the County Security Incident Response Team.

Incident Response

Responses can include or proceed through the following stages: identification, severity classification, containment, eradication, recovery and root cause analysis resulting in improvement of security controls. In the event of an incident, the Security Response Team shall take the following measures:

Contain, Eradicate, Recover and perform Root Cause Analysis

1. The IT Director shall implement containment procedures to prevent possible further data exposure. These include disabling all internet access to the network, disconnecting the device(s) from the network to prohibit communication, and implementing a freeze on all credit card processing.

2. The Finance Director shall notify applicable card associations.

   Visa

   Provide the compromised Visa accounts to Visa Fraud Control Group within ten (10) business days. For assistance, contact 1-(650)-432-2978. Account numbers must be securely sent to Visa as instructed by the Visa Fraud Control Group. It is critical that all potentially compromised accounts are provided. Visa will distribute the compromised Visa account numbers to issuers and ensure the confidentiality of entity and non-public information. See Visa's "What to do if compromised" documentation for additional activities that must be performed. That documentation can be found at:
   http://usa.visa.com/download/merchants/cisp-what-to-do-if-compromised.pdf

   MasterCard

   Contact the bank (the "merchant bank") which processes the County's credit and other payment card accounts for specific details on what to do following a compromise. Details on the merchant bank (aka. the acquirer) can be found in the Merchant Manual at http://www.mastercard.com/us/wce/PDF/12999_MERC-Entire_Manual.pdf.
   Your merchant bank will assist when you call MasterCard at 1-(636)-722-4100.

   Discover Card

   Contact your relationship manager or call the support line at 1-(800)-347-3083 for further guidance.

3. The Finance Director shall alert all necessary parties. Be sure to notify:

   a. Merchant bank

b. Local FBI Office
c. U.S. Secret Service (if Visa payment data is compromised)
d. Local authorities (if appropriate)

4. County General Council shall perform an analysis of legal requirements for reporting compromises in every state where clients were affected.

5. Collect and protect information associated with the intrusion. In the event that forensic investigation is required, the Chief Information Officer will work with legal and management to identify appropriate forensic specialists.

6. The IT Director shall eliminate the intruder's means of access and any related vulnerabilities. If necessary, compromised files will be restored from tape backups.

7. The IT Director shall research potential risks related to or damage caused by intrusion method used.

Root Cause Analysis and Lessons Learned

Not more than one week following the incident, members of the County Security Incident Response Team and all affected parties will meet to review the results of any investigation to determine the root cause of the compromise and evaluate the effectiveness of the *Incident Response Plan*. Review other security controls to determine their appropriateness for the current risks. Any identified areas in which the plan, policy or security control can be made more effective or efficient, must be updated accordingly.

Appendix C3 – Agreement To Comply

Agreement to Comply with Information Security Policies

All employees working with sensitive cardholder data must submit a signed paper copy of this form. Cumberland County management will not accept modifications to the terms and conditions of this agreement.

_____
Employee's Printed Name

_____
Employee's Department

_____
Employee's Telephone Number

_____
Employee's Physical Address and Mail Location

I, the user, agree to take all reasonable precautions to assure that Cumberland County internal information, or information that has been entrusted to Cumberland County by third parties such as customers, will not be disclosed to unauthorized persons. At the end of my employment or contract with Cumberland County, I agree to return to Cumberland County all information to which I have had access as a result of my position with Cumberland County. I understand that I am not authorized to use this information for my own purposes, nor am I at liberty to provide this information to third parties without the express written consent of the internal Cumberland County manager who is the designated information Owner.
I have access to a copy of the Cumberland County Information Security Policies Manual, I have read and understand the manual, and I understand how it impacts my job. As a condition of continued employment at Cumberland County, I agree to abide by the policies and other requirements found in that manual, as well as in any updates to that manual. I understand that non-compliance will be cause for disciplinary action up to and including system privilege revocation, dismissal from my employment with Cumberland County, and, perhaps, criminal and/or civil penalties.
I agree to choose a difficult-to-guess password as described in the Cumberland County Information Security Policies Manual, I agree not to share this password with any other person, and I agree not to write this password down unless it has been transformed in a way which makes it unrecognizable.

I also agree to promptly report all violations or suspected violations of information security policies to the Director of the Information Technology department.

_____
Employee's Signature

Appendix D1 – GUIDELINES FOR HAZARDOUS MATERIALS AND WASTE HANDLING

OSHA Hazard Communication Standard (HCS) Requirements

1. Hazardous materials in the workplace will be properly identified, labeled, and stored.

2. **Safety Data Sheets (SDS)** will be maintained for each product identified, reviewed and updated annually, and stored in a readily-accessible and labeled location.

3. Employees will be **provided initial and annual refresher training** regarding the:

   - presence of the specific materials;
   - potential physical and health hazards associated with those materials;
   - proper procedures for handling and using those materials, including the use of personal protective equipment (i.e., gloves and safety glasses);
   - location and use of the MSDS sheets; and
   - Procedures to be followed in the event of a release or other emergency.

EPA Hazardous Waste Management (HWM) Requirements

1. Hazardous wastes will be stored only in specific **satellite accumulation areas** (SAA's), which will be **designated with a sign** worded "Hazardous Waste Satellite Accumulation Area" or similar and by other appropriate means (i.e., marking tape on the floor or countertop). The SAA will be kept off-limits to anyone but authorized personnel, and be capable of being secured (locked).

2. Hazardous wastes will be collected only in **containers appropriate to the waste material, and segregated by compatibility**. The containers must be kept closed, stored on an impervious surface to prevent reaction or physical damage, and use secondary containment precautions. It is acceptable to transfer wastes from the point of generation to the storage containers with another, smaller container designated solely for that purpose (i.e., a labeled 1-gallon plastic jug of spent solvent). No more than 55-gallons or 200 kg of hazardous waste may be stored in a SAA at any one time.

3. The storage containers will be **labeled** as follows:

   - Name and EPA waste code of the material;

- Name (Cumberland County, Department name), address, location (building name and room #), and EPA generator number of the facility; and
- Start- and full-dates.

4. The SAA's will be **inspected daily while waste is present AND the work location is in use** by an authorized person for physical condition of the container(s) and signs of a release. Inspections are to be logged on the form provided, and the forms kept in or immediately adjacent to the SAA location. **When the location will be vacant for periods of time, the suspension and re-start dates will be noted on the log**. Any evidence of a release must be reported Facilities Office immediately.

5. Full SAA containers must be transferred to the main central accumulation area (CAA) within 72-hours, or scheduled for a separate vendor pickup, to meet the 90-day disposal requirement. Only sealed and labeled containers may be transferred from building to building. The wastes must be segregated by type, properly packaged and labeled, and manifested by the vendor on a form acceptable to the ME DEP.

6. The Safety Coordinator will supply signs, labels, and log forms, and initial and annual training of employees engaged in hazardous waste handling.

7. Specific handling requirements are outlined in the Cumberland County Hazardous Waste Management Plan.

Appendix D2 – ACCESS TO OCCUPATIONAL HEALTH RECORDS

ACCESS TO OCCUPATIONAL HEALTH RECORDS

According to OSHA Regulation 29 CFR 1910.1020(g), any employee has the right to see and copy:

1. His/Her medical records and any records of exposure to toxic substances or harmful physical agents in the workplace.

2. Records of exposure to toxic substances or harmful physical agents of other employees with work conditions, which are similar to his/hers.

3. Safety Data Sheets (SDS) or other information that exists for chemicals or substances used in the workplace, or to which employees may be exposed.

These records and a copy of 29 CFR 1910.1020 (g) is available at the following location:

Cumberland County
Office of Human Resources
142 Federal Street
Portland, Maine 04101

THIS NOTICE TO BE POSTED IN THE WORKPLACE HAZCOM STATION.

Appendix D3 – Global Harmonization Addendum

Format of the new Safety Data Sheets (SDS's)

Section 1, Identification includes product identifier; manufacturer or distributor name, address, phone number; emergency phone number; recommended use; restrictions on use.
Section 2, Hazard(s) identification includes all hazards regarding the chemical; required label elements.
Section 3, Composition/information on ingredients includes information on chemical ingredients; trade secret claims.
Section 4, First-aid measures includes important symptoms/ effects, acute, delayed; required treatment.
Section 5, Fire-fighting measures lists suitable extinguishing techniques, equipment; chemical hazards from fire.
Section 6, Accidental release measures lists emergency procedures; protective equipment; proper methods of containment and cleanup.
Section 7, Handling and storage lists precautions for safe handling and storage, including incompatibilities.
Section 8, Exposure controls/personal protection lists OSHA's Permissible Exposure Limits (PELs); Threshold Limit Values (TLVs); appropriate engineering controls; personal protective equipment (PPE).
Section 9, Physical and chemical properties lists the chemical's characteristics.
Section 10, Stability and reactivity lists chemical stability and possibility of hazardous reactions.
Section 11, Toxicological information includes routes of exposure; related symptoms, acute and chronic effects; numerical measures of toxicity.
Section 12, Ecological information*
Section 13, Disposal considerations*
Section 14, Transport information*
Section 15, Regulatory information*
Section 16, Other information, includes the date of preparation or last revision.

*Note: Since other Agencies regulate this information, OSHA will not be enforcing Sections 12 through 15(29 CFR 1910.1200(g)(2)).

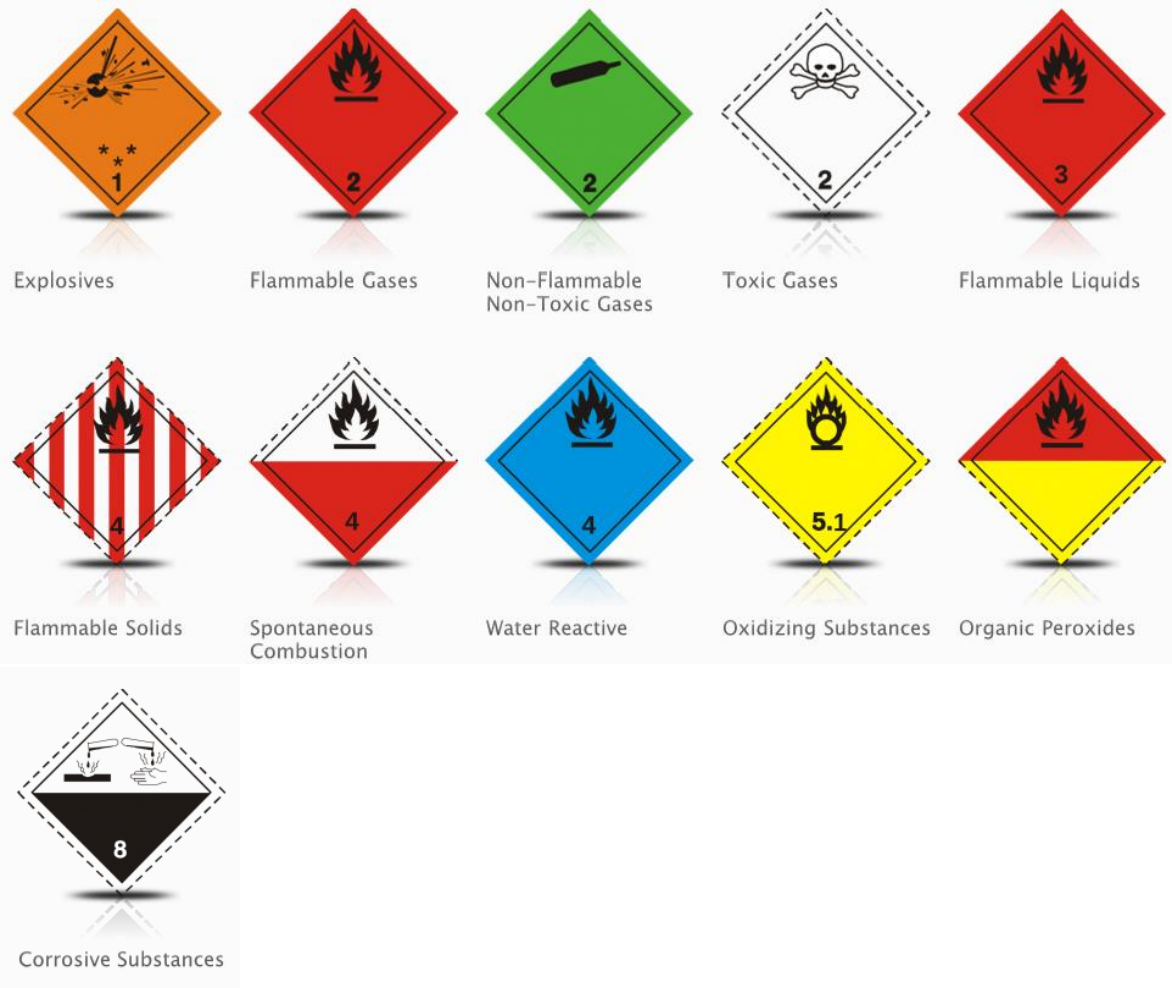
Appendix D4 – Pictograms

Health Hazards

Environmental Hazards

Physical Hazards

Transportation Hazards



Health Hazard

The red frame around the white diamond contains a black silhouette of a person's head and torso with a white star shape spreading through the chest area. This symbol indicates:

- Carcinogen
- Mutagenicity
- Reproductive Toxicity
- Respiratory Sensitizer
- Target Organ Toxicity
- Aspiration Toxicity

Gas Cylinder

The red frame around the white diamond contains a black shape like a rolling pin missing one handle. This symbol indicates:

- Gases Under Pressure

Flame Over Circle

The red frame around the white diamond contains a black circle resting on a black line with black flames on top of the black circle. It looks like the circle is on fire. This symbol indicates:

- Oxidizers

Flame

The red frame around the white diamond contains a white flame within black flames above a black line. This symbol indicates:

- Flammables
- Pyrophoric
- Self-Heating
- Emits Flammable Gas
- Self-Reactives
- Organic Peroxides

Corrosion

The red frame around the white diamond contains an image of two test tubes. One tube pours dripping liquid onto a solid black line, and the other tube drips liquid onto a hand. Both the solid line and hand image are eaten away where the liquids splash, emitting fumes. This symbol indicates:

- Skin Corrosion / Burns
- Eye Damage
- Corrosive to Metals

Environment
(Non-Mandatory for OSHA)

The red frame around the white diamond contains a black leafless tree silhouette and an upside-down fish image, both looking dead. This symbol indicates:

- Acute and/or chronic Aquatic Toxicity

Exclamation Mark

The red frame around the white diamond contains a large black exclamation point in the center. This symbol indicates:

- Irritant (skin and eye)
- Skin Sensitizer
- Acute Toxicity
- Narcotic Effects
- Respiratory Tract Irritant
- Hazardous to Ozone Layer (Non-Mandatory)

Exploding Bomb

The red frame around the white diamond contains a black round shape breaking apart with radiating black lines and fragments being ejected. This symbol indicates:

- Explosives
- Self-Reactive
- Organic Peroxides

- **Skull and Crossbones**

The red frame around the white diamond contains the image of a human skull with two bones crossed at an angle behind it. This symbol indicates:

- Acute Toxicity (fatal or toxic)

Appendix E1 – Sample Completed Grant Database Tracking Form

LINK: https://goo.gl/forms/MxGe193z3Jim66c23

GRANT DATABASE AND CENTRAL TRACKING PROGRAM

SAMPLE OF COMPLETED FORM

Email Address	luppi@cumberlandcounty.org
County Department	Executive
Department Grant Liaison	Faye Luppi
Granting Agency	Federal Government
Agency within Granting Entity	DOJ OVW
Program Name	Violence Intervention Partnership
Brief description of the grant's purpose	Supports a coordinated response to domestic violence/sexual assault in CC, provides services for underserved victims (incarcerated, rural, high risk, refugee/immigrant), and focuses on interventions for high risk cases: community supervision, High Risk Team, Judicial Monitoring, and Electronic Monitoring.
Grant number or other identifier	2015-WEAX-0016
Total funds	438,001
Length of Award	3 years
Date Awarded	9/25/2016
Date beginning	3/7/2016
Date ending	9/30/2018
Positions Supported or Created with Grant Funds?	Passthrough to another agency or agencies
How many positions?	4 .5 FTE positions plus OT for 1 more
County match, or other financial obligations to county?	N/A except inkind grant oversight
Reporting Dates	Jan 30 and July 30 every year
Extension deadline, if allowed	3/30/2019
Any notes, details, explanations of answers above?	
Grant Program Year	

Appendix FI – Grant Program Monitoring Policy

Grant Program Monitoring Policy

JANUARY 2021

Revised June 2021

TABLE OF CONTENTS

Introduction

Grants are subject to federal, state, and local government administrative requirements, cost principles, and audit requirements. The County of Cumberland ensures that subgrants are managed appropriately using a risk-based compliance assessment model and by performing analytical and financial compliance reviews. Grant Monitoring is comprised of monitors that assist subrecipients to ensure compliance with applicable regulations, laws, and grant subaward provisions. Items that monitors examine include:

- Organization operations
- Internal and management controls
- Grant subaward-related activities and expenditures
- Doing what was proposed and approved
- Meeting programmatic, administrative, fiscal requirements
- Consistency with the plan for programs/projects
- Identifying and resolving problems/issues
- Receiving needed technical assistance
- Federal Regulation compliance: EEOP, faith-based, civil rights, etc.

The four key components the County monitoring program model ensures:

1. Subrecipients are monitored during the term of the grant subaward;
2. Monitoring efforts focus on the areas of most significant risk;
3. All monitoring findings are addressed through appropriate corrective actions; and
4. Ongoing financial and administrative training and technical assistance is provided to subrecipients to enable them to comply with Grant Subaward requirements and maintain their funding.

The County of Cumberland uses the following methods to monitor subrecipient risk:

- **Day-to-Day Communication**: Grant Managers maintain ongoing communication with Subrecipients to provide programmatic guidance and review reimbursement requests. Because of Cumberland County's relatively small size, this will be far and away the most important monitoring method.

• **Desk Reviews:** Desk reviews test a subrecipient's fiscal and administrative compliance with laws, regulations, and program guidelines via desk reviews. Desk reviews allow the subrecipients to make certain assertions regarding various aspects of their operations, or provide monitors an opportunity to verify the allowability of expenditures charged to the grant subaward. These reviews consist of, but are not limited to, the following:

a. Compliance reviews of Progress Reports against the subrecipient's proposal plan of action and follow-up corrective action, if required;

b. Payment reviews of invoices and other documents supporting cash requests claimed by and made to the subrecipient;

c. Follow-up site visits to verify implementation of required corrective action. The scope of the review can be expanded if needed.

• **Site Visits**: Grant Managers conduct periodic site visits to review a subrecipient's overall implementation of the program, adherence to program guidelines, and achievement of grant subaward goals and objectives and to identify issues and provide technical assistance as needed.

Site Visits will be scheduled yearly, preferably during March or September. This does not exclude the opportunity for site visits at other times.

Each funded grant project (also known as subrecipient) has been assigned to a County Grant Manager, who will serve as the program's primary contact. The primary contact is the individual responsible for scheduling and conducting the Site Monitoring Visit as well as for providing technical assistance to the program. The Cumberland County Finance Department will participate in the Site Visit as described in the site monitoring agreement. The primary contact is responsible for scheduling, main inquiries, and writing of the programmatic portion of the Site Monitoring Report.

The Grant Manager will schedule Site Monitoring visits on a random basis once every two years for each subgrant except for projects receiving less than $25,000 in total from the

County. Projects receiving less than $25,000 may be subject to a desk review or a site monitoring visit.

While the Cumberland County GPMP is intended for Countywide use, it also not intended to supersede the policies of the Community Development Block Grant program of the County, which is also involved in a variety of other Housing and Urban Development (HUD) grants. Their monitoring program is similar to the County Policy, but also goes beyond other County requirements due to the HUD guidelines.

Glossary of Terms and Acronyms

Corrective Action Plan ..... A corrective action plan (CAP) is a step by step plan of action that is developed to achieve targeted outcomes for resolution of identified errors in an effort to: (1) identify the most cost-effective actions that can be implemented to correct error causes, (2) achieve measurable improvement in the highest priority areas and, (3) eliminate repeated deficient practices

Compliance Review ..... An evaluation by Cumberland County staff to assess a subrecipient's business and financial management systems to ensure that regulations and policies are being followed.

EEOP ..... Equal Employment Opportunity Plan

Finding ..... A finding is an operational deficiency in internal controls, noncompliance with provisions of laws, regulations, contract terms, grant subawards, or fraud, waste and abuse.

Monitoring ..... Both the broad overall system of reviewing and tracking the use of subgrant funds, and the more specific day-to-day review processes to assure that a subrecipient is complying with federal or state rules and regulations, and is meeting the goals and objectives of the subgrant.

Risk Assessment....Periodic assessments of the risk level of Subrecipients, intended to provide initial guidance as to the level of monitoring needed.

Subaward ..... A grant provided by a pass-through entity (Cumberland County) to a subrecipient for the subrecipient to carry out part of a Federal award received by the pass-

through entity. It does not include payments to a contractor or payments to an individual that is a beneficiary of a Federal program. A subaward may be provided through any form of legal agreement, including an agreement that the pass-through entity considers a contract.

Subrecipient ..... Entity that receives a subaward from a pass-through entity to carry out part of a Federal program; but does not include an individual that is a beneficiary of such program. A subrecipient may also be a recipient of other Federal awards directly from a Federal awarding agency.

Annual Compliance Monitoring Plan

The Annual Compliance Monitoring Plan identifies the proposed subrecipients eligible for a compliance review for the year. Although the priority is to review subrecipients identified as high-risk, Cumberland County will also conduct reviews of subrecipients with low risk scores

COMPLIANCE REVIEW PROCESS

The objective of a compliance review is to ensure the subrecipient complies with the Code of Federal Regulations, applicable state laws, and other governing regulations, internal policies, and general good business practices. The compliance review process is outlined below:

- **Notification Letter**: The compliance review continues with the issuance of a notification letter. The purpose of this letter is to notify the head of the organization or subrecipient in writing that a compliance review will be conducted. The letter identifies the date of fieldwork, grant(s) selected for review, and scope of the review.
- **Request for Documentation**: A request for documentation is included with the notification letter. The purpose of the request for documentation is to request specific documents that should be made available for review. These records might include, but are not limited to, contracts, invoices, procurement records, indirect costs methodology, and personnel ledger, including timesheets and supporting documentation to support match.
- **Risk Assessment**: The County of Cumberland will annually update Risk Assessments of Subrecipients. For Subrecipients judged to be low-risk, the

compliance review can end at this step, but also may continue on to a site visit. For Subrecipients judged to be high-risk, the review process will continue to the next step.

• **Site Visits:** During the Site Visits, monitors are present at the subrecipient's physical location gathering, analyzing, and evaluating evidence to assess and verify they are complying with federal and state regulations. The monitoring team will be comprised of the Grant Manager and possible Finance Department staff. During the fieldwork, the monitors can provide technical assistance, if needed, while addressing areas of non-compliance. In addition, the monitoring team can also provide technical assistance based on their subject matter knowledge and reference to best practices during the site visits.

Report Timeliness: All compliance review reports will be issued within 90 days of the last day of fieldwork. Additional coaching notes are written when the compliance report needs revision or corrections. The compliance review report remains open until the subrecipient submits their Corrective Action Plan (CAP) if applicable.

Compliance Review Report: The next step is to issue the compliance review report to the subrecipient including senior management and key administrative staff. The report outlines all non-compliance issues and findings, provides recommendations for improvement and may request the subrecipient generate a CAP.

Recommendations: A recommendation must provide a course of action that will correct a finding or issue that has been identified and provide improvements. Recommendations should be action-oriented, convincing, well-supported, and effective.

Questioned Costs: A questioned cost can result from a violation, or possible violation, of a statute, regulation, or the terms and conditions of a grant subaward. In addition, it could be a cost not supported by adequate documents, or appears unreasonable and does not reflect the actions a prudent subrecipient would take in the circumstances.

Disallowed Costs: A disallowed cost is a charge that the pass-through entity determines to be unallowable per the Code of Federal Regulations or the County of Cumberland purchasing policy. Some examples of disallowed costs can be the purchase of alcohol, lobbying, or costs pertaining to waste, fraud, and abuse.

CAP: Once the subrecipient receives the compliance review report, they will have 30 days to either dispute the findings or provide a CAP to correct and address any finding(s), or send payment of a disallowed cost. After a CAP is received, the subrecipient has six months from the date of the reply to implement the CAP. If necessary, follow-up reviews will be conducted by Cumberland County to ensure that corrective actions are implemented in a timely manner.

If a subrecipient fails to comply with the required necessary corrections identified, funding may be suspended until corrections are completed. Failure to comply with grant requirements may subject the subrecipient to Special Conditions of future funding opportunities or the subrecipient may be required to provide a reimbursement.

Closing Letter: Once the CAP is received and the subrecipient has satisfactorily addressed and/or corrected all findings, the Grant Manager will issue a closing letter informing the subrecipient that the compliance review is closed.

Appeals Process: If the subrecipient does not agree with the finding, they have 30 days from the date the compliance review report is issued to dispute the finding in writing and provide additional supporting documentation. If the finding is not cleared with the additional information provided, a notification letter will be issued. The subrecipient may appeal the decision to the department within 30 days of the notification letter. The final decision on any appeal rests with the County Manager.

Scheduling a Site Monitoring Visit

The primary contact will schedule a routine Site Monitoring Visit at least two weeks in advance by contacting the Grant Manager to:

• Schedule the date and time of the Site Monitoring Visit (include arrival time and approximate length)

• Designate staff to be interviewed (at minimum, the Project Director, Fiscal Officer, and grant funded staff);

- The Grant Manager will create an agenda for the Site Monitoring Visit.
    - The agenda will include approximate times to meet with different staff, materials that will be reviewed with these staff members, and topics of discussion.
    - The Grant Manager will provide this agenda to the Project Director via e-mail prior to the Site Monitoring Visit, allowing time for the Project Director to review the agenda and suggest revision(s).

• Outline the need for access to program and fiscal files and documents.

o For victim service organizations, personally identifying information will need to be redacted from the files prior to the SM Visit to protect any identifying information.

• Inform the Project Director that additional items may be requested at the time of the Site Monitoring Visit.

• Assess the need to plan technical assistance during the Site Monitoring Visit.

Internal Review prior to Site Monitoring Visit

Prior to the Site Monitoring Visit, the Grant Monitoring Staff will review materials submitted by the subrecipient to the County using the Grant Monitoring Checklist. Following is a list of items to be included in the review process, as well as questions to assist the County Staff in their analysis of the materials.

Program's file: funding application; performance reports; correspondence & previous site monitoring report.

• Are there any clarifications that need to be made? If so, what?

• Are more details needed? If so, what?

• Any "red flags"?

• Any difficulties the project is encountering?

- Weaknesses of the project?
- Strengths of the project?
- Compliance with certified assurances issues?
- Are timelines being met?
- Are the DUNS # and SAM Registration current?

Program's fiscal information: overall budget, reimbursement claims, any budget revision requests, any key purchases with grant funds or matching funds

- Are there any clarifications that need to be made? If so, what?
- Are more details needed? If so, what?
- Any "red flags"?
- Are timelines being met?
- Ask the Finance Department representative about any concerns.

After reviewing the above items and considerations, the Grant Manager will create a list of questions and concerns for the Site Visit using the Checklist.

Appendix F2 – Personally Identifiable Information (PII)

1. PREVENTION OF BREACH OF PERSONALLY IDENTIFIABLE INFORMATION

The County actively protects personally identifiable information (PII) from access by, or disclosure to, unauthorized individuals. The purpose of this document is to reiterate policy and establish standardized response and notification procedures for breaches of that policy. In the event of a breach in PII, County personnel are to comply with the following procedures for response and notice to affected individuals and Federal agencies. These policies and procedures govern breaches by County personnel that may result in unauthorized access, internal or external to the County, whether involving electronic systems or paper documents.

2. TERMINOLOGY

The policy applies to a breach of personally identifiable information (PII), which is a type of incident. For the purposes of this policy, the definitions in this section apply.

- **Personally identifiable information (PII)** means 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. (i.e., a person's name in combination with any of the following information, such as relative's names, postal address, personal e-mail address, home or cellular telephone number, personal characteristics, Social Security number (SSN), date or place of birth, mother's maiden name, driver's license number, bank account information, credit card information, or any information that would make the individual's identity easily discernible or traceable).

- **Breach**, as directed by OMB Memorandum M-17-12, is defined as the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses personally identifiable information for an other than authorized purpose.

  A breach is not limited to an occurrence where a person other than an authorized user potentially accesses PII by means of a network intrusion, a targeted attack that exploits website vulnerabilities, or an attack executed through an email message or attachment.

  A breach may also include the loss or theft of physical documents that include PII or portable electronic storage media that store PII, the inadvertent disclosure of PII on

a public website, or an oral disclosure of PII to a person who is not authorized to receive that information. It may also include an authorized user accessing PII for other than an authorized purpose.

Some common examples of a breach include:

- A laptop or portable storage device storing PII is lost or stolen;
- An email containing PII is inadvertently sent to the wrong person;
- A box of documents with PII is lost or stolen during shipping;
- An unauthorized third party overhears agency employees discussing PII about an individual seeking employment or Federal benefits;
- A user with authorized access to PII data sells it for personal gain or disseminates it to embarrass an individual;
- An IT system that maintains PII is accessed by a malicious actor; or
- PII that should not be widely disseminated is posted inadvertently on a public website.

- **Incident** refers to **a**n occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

3. REPORTING REQUIREMENTS

The County must report an actual or imminent breach of PII to a Program Manager of the appropriate Federal grant awarding agency, for example, the Department of Justice Offices of Justice Programs or Violence Against Women, no later than 24 hours after an occurrence of an actual breach, or the detection of an imminent breach. [1]

The procedures should promote cooperation and the free exchange of information with Federal awarding agency officials, as needed, to properly escalate, refer, and respond to a breach.

The County Manager is ultimately responsible for deciding whether to provide notification on behalf of the County, offer guidance, and provide services to individuals potentially affected by a breach. When a contractor provides notification on behalf of an agency, such

[1] **Grant Award Requirements:** The grantee must have written procedures in place to respond in the event of an actual or imminent "breach" (OMB M-17-12) if it (1) creates, collects, uses, processes, stores, maintains, disseminates, discloses, or disposes of "personally identifiable information (PII)" (2 CFR 200.79) within the scope of an OJP grant-funded program or activity, or (2) uses or operates a "Federal information system" (OMB Circular A-130). The breach procedures must include a requirement to report actual or imminent breach of PII to an OJP/OVW Program Manager no later than 24 hours after an occurrence of an actual breach, or the detection of an imminent breach.

activities shall be in accordance with OMB guidance and the agency's breach response plan and shall be coordinated with and subject to prior written approval by the head of the agency.

The County requires all individuals with access to the agency's information systems to report a suspected or confirmed breach to the County Compliance and Auditing Manager as soon as possible and without unreasonable delay. Such individuals shall not wait for confirmation that a breach has in fact occurred before reporting, as such a delay may undermine the agency's ability to apply preventative and remedial measures to protect the PII or reduce the risk of harm to potentially affected individuals. In addition, any delay may reduce the likelihood that the agency can recover a lost or stolen device or physical document.

Subawardees of the County shall report any breach of PII to the County Compliance and Auditing Manager, who shall then follow the procedures outlined in this section.

4. ASSESSING RISK OF HARM TO INDIVIDUALS POTENTIALLY AFFECTED BY A BREACH:

In order to properly tailor breach response activities, the County Compliance and Auditing Manager shall conduct and document an assessment of the risk of harm to individuals potentially affected by a breach, including consideration of the potential harms that could result from the loss or compromise of PII. Such harms may include the effect of a breach of confidentiality or fiduciary responsibility, the potential for blackmail, the disclosure of private facts, mental pain and emotional distress, financial harm, the disclosure of contact information for victims of abuse, the potential for secondary uses of the information which could result in fear or uncertainty, or the unwarranted exposure leading to humiliation or loss of self-esteem.

5. FACTORS FOR ASSESSING THE RISK OF HARM TO POTENTIALLY AFFECTED INDIVIDUALS.

At a minimum, the County Compliance and Auditing Manager shall consider the following factors when assessing the risk of harm to individuals potentially affected by a breach:

- Nature and sensitivity of the PII potentially compromised by the Breach, including the potential harms an individual could experience from the compromise of that type of PII;
- Likelihood of Access and Use of PII;
- Type of Breach, including the circumstances of the breach, as well as the actors involved and their intent.

6. MITIGATING THE RISK OF HARM TO INDIVIDUALS POTENTIALLY AFFECTED BY A BREACH.

Once the County Compliance and Auditing Manager assesses the risk of harm to individuals potentially affected by a breach, the County shall consider how best to mitigate the identified

risks. The County Compliance and Auditing Manager is responsible for advising the County Manager on whether to take countermeasures, offer guidance, or provide services to individuals potentially affected by a breach. Because each breach is fact-specific, the decision of whether or not to offer guidance or provide services to individuals will depend on the circumstances of the breach. When deciding whether or not to offer guidance or provide services to potentially affected individuals, the County shall consider the assessed risk of harm.

7. NOTIFYING INDIVIDUALS POTENTIALLY AFFECTED BY A BREACH.

The County Compliance and Auditing Manager is responsible for advising the County Manager on whether and when to notify individuals potentially affected by a breach. Because each breach is fact-specific, the decision of whether or not to notify individuals will depend on the circumstances of the breach. When deciding whether or not to notify individuals potentially affected by a breach, agencies shall consider the assessed risk of harm. The assessed risk of harm to individuals shall inform the County's decision of whether or not to notify individuals. The County Manager is ultimately responsible for making a final decision regarding whether to provide notification.

Whether and how to notify potentially affected individuals must also:

- Take into account survivors' safety and privacy;
- Not breach survivor confidentiality;
- Reasonably inform survivors whose data has been breached so they can take measures to minimize the harm that may have been caused by the breach.

8. TRACKING AND DOCUMENTING THE RESPONSE TO A BREACH.

The County shall develop and maintain a formal process to track and document each breach reported to the agency. The process shall ensure that the County Compliance and Auditing

Manager is made aware in a timely manner of each report of a suspected or confirmed breach. When the County Compliance and Auditing Manager determines that the agency's response to a breach has concluded, the County Compliance and Auditing Manager shall report that status to the County Manager along with the outcome of the response.

Appendix F3 – Response to workplace-related incidents of sexual misconduct, domestic violence and dating violence

I. Purpose

Cumberland County commits to a safer and more supportive organizational climate and to the prevention and reduction of the incidence and effects of domestic violence, sexual violence, and stalking [hereinafter "violence"] at the workplace.

II. Definitions

1. Survivor or victim: an individual who is currently subject to, or has in the past been subjected to, domestic violence, sexual violence, stalking or other forms of violence.
2. Perpetrator: An individual who commits or threatens to commit an act of domestic violence, sexual violence, or stalking.
3. Domestic violence: a pattern of coercive behavior, including acts or threatened acts, that is used by a perpetrator to gain power and control over a current or former spouse, family member, intimate partner, or person with whom the perpetrator shares a child in common. Domestic violence includes, but is not limited to: physical violence, injury, or intimidation; sexual violence or abuse; threats; harassment; or stalking.
4. Sexual violence: a range of behaviors, including but not limited to: sexual harassment; a completed nonconsensual sex act (i.e. rape); an attempted nonconsensual sex act; abusive sexual contact (i.e. unwanted touching); and noncontact sexual abuse (e.g., threatened sexual violence, exhibitionism, verbal harassment). Some or all of these acts may also be addressed in Cumberland County's Sexual Harassment policy. Sexual violence is any sexual act or behavior that is perpetrated against someone's will when someone does not or cannot consent.
5. Stalking: refers to harassing, intimidating or threatening conduct that causes the survivor to fear for his or her safety or the safety of a family member, or would cause a reasonable person in a similar situation to fear for his or her safety. Stalking conduct includes, but is not limited to: following or spying on a person; appearing at a person's home or work; engaging in unwanted, harassing, or threatening phone calling, emailing, texting, etc.; and posting information or spreading rumors about the survivor on the internet, or in a public place. Stalking may occur through use of technology including, but not limited to: email; voicemail; text messaging; and use of social networking sites.
6. Workplace-Related incidents of domestic violence, sexual violence, dating violence, and stalking: include acts, attempted acts or threatened acts by or against employees, the families of employees, and/or their property, that imperil the safety

or well-being of any person associated with an employee of Cumberland County, regardless of whether the act occurred in or outside the organization's physical workplace. An employee is considered to be in the workplace while in, or utilizing the resources of the employer, including but not limited to facilities, work sites, equipment, or vehicles, or while on work-related travel.

III. Persons Covered by this Policy

Persons covered by this policy include full and part-time employees, interns, contractors, volunteers or temporary workers engaged by Cumberland County that are grant-funded or supported personnel by the 2021-2024 OVW ICJR grant #15JOVW-21-GG-02024-ICJR in any workplace location.

IV. Statement of Confidentiality

Cumberland County recognizes and respects an employee's right to privacy and the need for confidentiality and autonomy. Cumberland County shall maintain the confidentiality of any employee's disclosure regarding violence to the extent allowed by law, and unless to do so would result in physical harm to any person, and/or jeopardize safety within the workplace. When information must be disclosed to protect the safety of individuals within the workplace, Cumberland County shall limit the breadth and content of such disclosure to information reasonably necessary to protect the safety of the disclosing employee and others, and to comply with the law. Cumberland County shall provide advance notice to the employee who disclosed information, to the extent possible, if the disclosure must be shared with other parties in order to maintain safety in the workplace or elsewhere.

V. Employer Responses to Violence

A. Responses to Survivors

i. *Non-Discrimination and Non-Retaliation*: Cumberland County will not discharge or in any manner discriminate or retaliate against an employee solely because of the employee's status as a survivor of domestic violence, sexual violence, or stalking, if the survivor provides notice to the organization of the status, or the organization has actual knowledge of the status.

Cumberland County will not retaliate against a survivor of domestic violence, sexual assault, or stalking for requesting leave or a reasonable accommodation, regardless of whether the request was granted.

ii. *Leave, other Reasonable Accommodations and Assistance, and Work Performance:* Cumberland County recognizes that survivors of domestic violence, sexual assault, stalking and dating violence may need time off to obtain or attempt to obtain a protection order or other legal assistance to help ensure his or her health, safety, or

welfare of that of his or her child. The County will work in collaboration with the employee to provide reasonable and flexible leave options when an employee or his or her child is a survivor of domestic violence, sexual assault, and/or stalking.

An employee must provide reasonable advance notice to the employer of the need to take time off unless advance notice is not feasible. Cumberland County may require the employee to provide documentation or other certification verifying that the employee was a survivor of violence.

Cumberland County will also provide reasonable accommodations for a survivor of domestic violence, sexual violence, or stalking who requests an accommodation for the safety of the survivor or to maintain his or her work performance while at work. Reasonable accommodations may include the implementation of safety measures, including a modified schedule, changed work telephone or work station, assistance in documenting the violence that occurs in the workplace, an implemented safety procedure, or referral to a survivor advocacy or assistance organization. Cumberland County will assist an employee to enforce his or her protection order, if applicable. *See also Personnel Policy, Appendix B, Domestic Violence*

B. Responses to Workers Who Commit Violence

If Cumberland County receives information that alleges or suggests that an employee has committed an incident of workplace-related violence, then the matter shall be referred to the designated executive for the purpose of investigating the information or allegation.

At the conclusion of the investigation conducted by Cumberland County, the investigator shall report her or his findings to the designated official. If the investigator concludes, by a preponderance of the evidence, that the employee has engaged in a workplace-related incident, as defined in this Policy, then that employee shall be subject to disciplinary action up to and including termination. The employee might also be required to participate in counseling or other remedial measures.

An employee who is subject to a protection order, or a named defendant in a criminal action as a result of a threat or act of domestic violence, sexual violence, or stalking, must notify the Cumberland County Human Resources Department immediately regarding the existence of such criminal or civil action. Failure to disclose the existence of such criminal or civil actions in these circumstances will result in disciplinary action, up to and including termination from employment.

VI. Reporting by Employees Who are Survivors

Employees who are survivors of domestic violence, sexual assault, and stalking are encouraged to provide a report to Cumberland County. Cumberland County has designated the Human Resources Director as the person to whom such reports should be made. This designated employee shall provide community referrals and resources to employees in order to assist employees with their concerns or experiences regarding violence.

VII. Resources

Employees who wish information or assistance are encouraged to reach out to any resources below.

Through These Doors, www.throughthesedoors.org; Free, 24 Hour Confidential Helpline 1-800-537-6066

Sexual Assault Response Services of Southern Maine, www.sarsonline.org; Free, 24 Hour Confidential Helpline 1-800-871-7741

Immigrant Resource Center of Maine, ircofmaine.org; https://www.ircofmaine.org/how-to-get-gender-based-violence-help.html

Pine Tree Legal Assistance, https://www.ptla.org/family-law-and-victim-rights-unit

A Different Choice, https://www.throughthesedoors.org/violence-intervention/; a Certified Domestic Violence Intervention Program (CDVIP) for men who perpetrate domestic violence, facilitated by trained educators

Choices- The Men's Group Certified Domestic Violence Intervention Program, Brunswick, ME; (207) 240-4846

Appendix G1– Grant Authorization Form

STEP 1- (to be filled out by Project Manager)

☐ New Completed Request ☐ Continuation ☐ Amendment to Grant ☐ Initial Notification

Materials to follow

ATTACH A COPY OF GRANT APPLICATION WITH DETAILED BUDGET.

Name of Grant: _____

Department requesting grant: _____

Project Manager: _____

Briefly state purpose: _____

Proposed grant time period: _____

Match required? $_____

Money in your budget? If so, where? _____

Long Term Budget Cost? Yes/No Approximate Annual Budget Impact?_____

Department Director signature: _____

Turn into County Treasurer.

_____

STEP 2- (to be filled out by County Treasurer)

1. Is everything in order? ____YES/NO_____

2. Funding Proposal acceptable? _____YES/NO_____

3. Unique identifier assigned to grant (for tracking purposes only): _____

Signature of County Treasurer_____ Date: _____

Forward to Grant Oversight Committee

_____

STEP 3

☐ Approved to commence with the application process

Or

☐ Needs Commissioner review and acceptance to submit

_____ _____

County Manager Date

If the grant is awarded, you must submit award letter and contract to the County Manager. Go to STEP 4

STEP 4

The Grant has been awarded. You are authorized to commence with the scope of the grant received

_____ _____

County Manager Date