



CITY OF KINGSLAND, GEORGIA

CITY COUNCIL

AGENDA • APRIL 23, 2018

Regular Meeting

City Council Chamber

6:00 PM

107 South Lee Street - City Hall, Kingsland, GA 31548

I. PUBLIC HEARING - STARTS AT 6:00PM

1. Public Hearing for an Application for a Temporary Special Event Permit. Application is for a One Day Alcohol Beverage License from McGarvey's Wee Pub, 2603 Osborne Road, St. Marys, Georgia 31558 to Serve Alcohol at the Downtown K-Bay Street Fair on May 12, 2018. -
2. Public Hearing on Zoning Text Amendment of Zoning District C-1 Central Business District (CBD) and the Addition of C-1A Commercial Corridor District (CCD) Along with Regulations Regarding Uses and Restrictions. -
3. Public Hearing on the "Draft" Camden County Joint 2018-2028 Comprehensive Plan. the Draft Document Will be Available for Public Inspection on March 29, 2018 in the Kingsland City Clerk's Office. -

II. CALL TO ORDER AND WELCOME GUESTS

III. INVOCATION AND PLEDGE TO THE FLAG

1. Reverend Al Crumpton, King of Peace Episcopal Church -

IV. ROLL CALL

Kenneth E Smith Sr
James McClain
Charles Grayson Day Jr.
James W Galloway
Michael J McClain

Mayor
Mayor Pro Tem
Councilman
Councilman
Councilman

V. CONSENT DOCKET

- A. Approve the Council Minutes of the last regular Council Meeting
- B. Approve the Agenda as Presented
- C. Approve the Payments of Accounts Payable as Due and Funds Available

VI. RECOGNITION

1. Recognizing Georgia Cities Week Sponsors -
2. Recognizing Volunteers from City of Kingsland's Boards -

VII. PRESENTATION

1. City of Kingsland FY 2016-17 Audit Presentation by City Auditor, David Irwin, CPA of Mauldin & Jenkins, LLC -

VIII. GRANTING AUDIENCE TO THE PUBLIC**IX. OLD BUSINESS****X. PLANNING AND ZONING**

1. Approval Of: Zoning Text Amendment , Downtown Overlay District -

The City of Kingsland Planning Commission has recommended the amending of zoning district C-1 Central Business District (CBD) and the addition of C-1A Commercial Corridor District (CCD) along with regulations regarding uses and restrictions. Planning Commission Recommends Approval.

2. Approval Of: Camden County Joint Comprehensive Plan - 2018-2038 -
3. Adoption Of: Resolution #2018-09 -

Resolution to Transmit the Joint Comprehensive Plan of the City of Kingsland to the Coastal Regional Commission and The State of Georgia Department of Community Affairs.

XI. NEW BUSINESS

1. Approval Of: Temporary/Special Event Permit for McGarvey's Wee Pub -

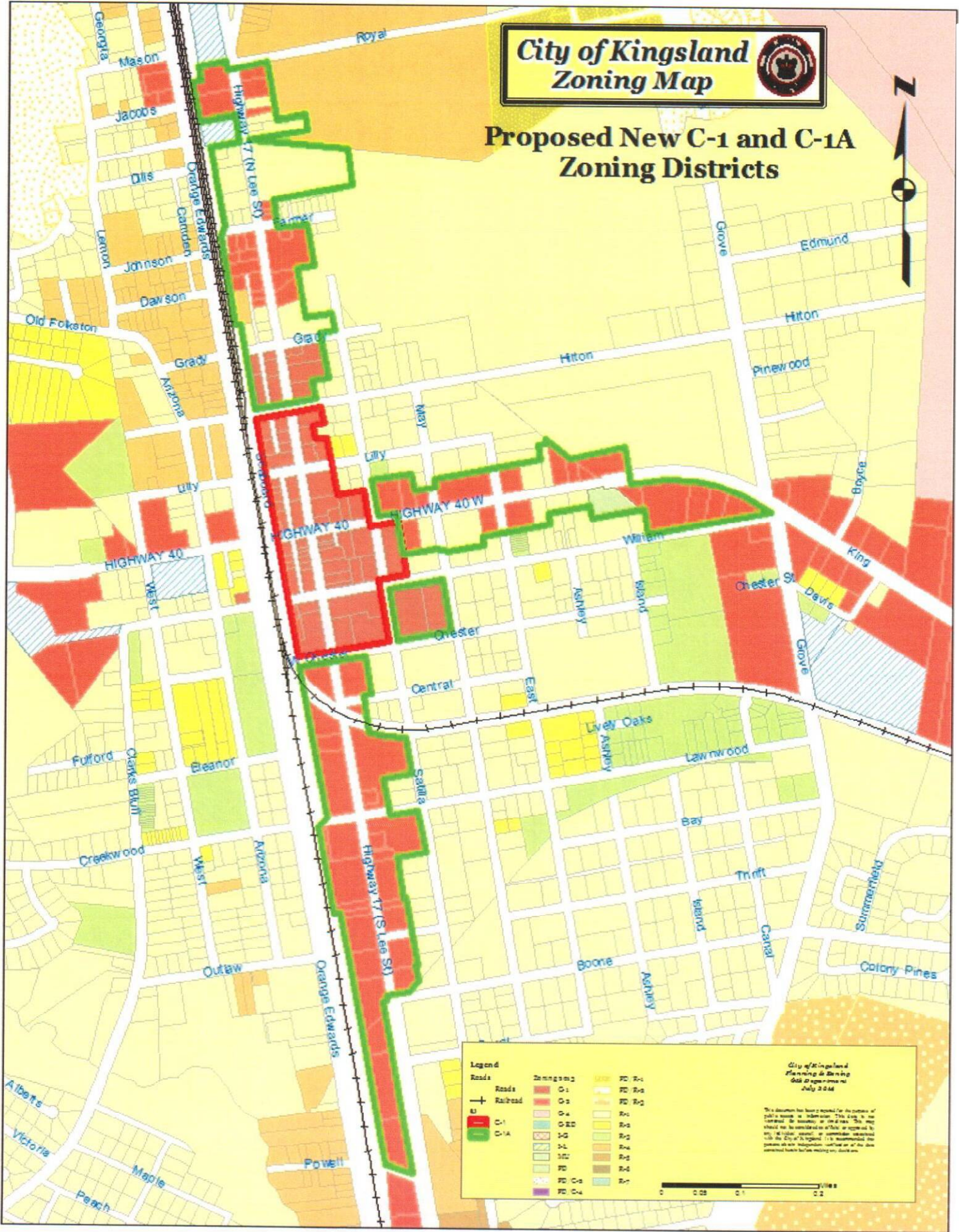
This temporary/special event permit is to serve alcohol at the downtown K-Bay Street Fair to take place in downtown Kingsland, Georgia on May 12, 2018.

2. 2128 : Approval Of: Quit Claim Deed, Harriett's Bluff Road Lift Station -
Staff recommends approval.

3. Approval Of: Policies for GCIC Compliancy for Kingsland Fire Department -

XII. MAYOR AND COUNCIL ANNOUNCEMENT

XIII. ADJOURNED



**RESOLUTION TO TRANSMIT
THE JOINT COMPREHENSIVE PLAN OF THE CITY OF KINGSLAND TO
THE COASTAL REGIONAL COMMISSION AND
THE STATE OF GEORGIA DEPARTMENT OF COMMUNITY AFFAIRS**

WHEREAS, The City of Kingsland, Georgia is an incorporated jurisdiction Camden County; and,

WHEREAS, The City of Kingsland is subject to the State of Georgia Planning Act of 1989 which call for a certified Comprehensive Plan in order to obtain and maintain the status of Qualified Local Government; and,

WHEREAS, The City of Kingsland is a member of the Coastal Regional Commission, an agency created to provide regional planning and intergovernmental coordination among certain county and city governments in the coastal area of Georgia; and,

WHEREAS, The City of Kingsland initiated a process to complete the Joint Comprehensive Plan 2018-2038 with an initial public hearing held on October 10, 2017, to brief the community on the process to be used to develop the plan, opportunities for public participation in development of the plan, and to obtain input on the proposed planning process; and,

WHEREAS, in order to adopt a Joint Comprehensive Plan meeting the requirements of law, and to maintain Qualified Local Government status, The City of Kingsland has prepared a document being labeled and described as the City of Kingsland Comprehensive Plan 2018-2038, has held the required public hearings, and now must transmit this document to the Coastal Regional Commission and the State of Georgia Department of Community Affairs for review in accordance with procedures prescribed by state law; and,

WHEREAS, The City of Kingsland Joint Comprehensive Plan 2018-2038 was prepared according to the Standards and Procedures for Local Comprehensive Planning established by the Georgia Planning Act of 1989, and includes the community's certification that consideration was given to both the Regional Water Plan and the Georgia Department of Natural Resource Rules for Environmental Planning Criteria as provided in Section 110-12-1-.0293) of the above-mentioned Standards and Procedures in preparing the plan, that the required second public hearing was held February 26, 2018;

NOW, THEREFORE, BE IT RESOLVED BY THE MAYOR AND COUNCIL OF THE CITY OF KINGSLAND, GEORGIA, AND IT IS HEREBY RESLOVED that The City of Kingsland Joint Comprehensive Plan 2018-2038 be transmitted to the Georgia Coastal Regional Commission and the Georgia Department of Community Affairs for official review as required by the rules governing the Planning Act of 1989.

BE IT FURTHER RESOLVED, that the resolution herein authorizes transmittal as prescribed effective this 9th day of April, 2018.

APPROVED FOR TRANSMITTAL

Kenneth Smith Sr., Mayor

ATTEST:

Linda O' Shaughnessy, City Clerk

Attachment: RESOLUTION TO TRANSMIT (3) (2136 : Adoption Of: Resolution #2018-09)



City of Kingsland Georgia

P.O. BOX 250, Kingsland, Georgia 31548
PHONE 912 729-5613 FAX 912 729-4590

NOTICE OF PUBLIC HEARING ALCOHOL BEVERAGE LICENSE (TEMPORARY/SPECIAL EVENT PERMIT)

The City Of Kingsland, Georgia has received an application for a one day alcohol beverage license from, "McGarvey's Wee Pub" 2603 Osborne Road St Marys, Georgia 31558, to serve alcohol at the downtown K-Bay Street Fair. This event will take place downtown Kingsland Georgia May 12, 2018. Notice is hereby given that a public hearing on this application is scheduled for Monday, April 23, 2018 at 6:00 p.m. in the council chamber at City Hall 107 South Lee Street.

Anyone having any objection to the issuance of a license to this establishment should address their concern to the Mayor and Council at the public hearing. Formal consideration of this application will take place during the regular council session on Monday, April 23, 2018.

Yvonne Waye, Community Planning & Development Administrator

Please Advertise:

April 19, 2018

Attachment: temp alcohol license (2131 : Approval Of: Temporary/Special Event Permit for McGarvey's Wee Pub)

STATE OF GEORGIA

COUNTY OF CAMDEN

QUIT CLAIM DEED

THIS INDENTURE, made this 6 day of April 2018 by and between S.W.S., L.L.C., a Georgia Limited Liability Company with principal offices in Glynn County, Georgia, herein referred to as party of the first part, and CITY OF KINGSLAND, a municipal corporation created under the laws of the state of Georgia, herein referred to as the party of the second part.

WITNESSETH

That the said party of the first part, for and in consideration of the sum of One (1) Dollar and as agreed to in the construction and reimbursement agreement between all parties dated December 20, 2004, does hereby remise, convey, and forever QUIT-CLAIM to the said party of the second part, its successors and assigns all that lot, tract, or parcel of land lying and being in Camden County, Georgia, more particularly described as follows:

All that tract or parcel of land lying and being in the 31st G.M. District, Camden County, Georgia, being a portion of parcel "C" (according to survey for C. P. Sapp, L.L.C., recorded in plat drawer 17, map number 52, public records of said county) and being more particularly described as follows:

FOR A POINT OF REFERENCE COMMENCE AT A POINT LYING ON THE SOUTHEASTERLY RIGHT-OF-WAY LINE OF HARRIETTS BLUFF ROAD (A VARIED WIDTH RIGHT-OF-WAY, ACCORDING TO GEORGIA DEPARTMENT OF TRANSPORTATION PROJECT NO. 1-95-1(11)00), SAID POINT BEING THE MOST WESTERLY CORNER OF SAID PARCEL "C" AND RUN THENCE NORTH 58°-22'-50" EAST, ALONG SAID SOUTHEASTERLY RIGHT-OF-WAY LINE, A DISTANCE OF 142.59 FEET TO A POINT; RUN THENCE NORTH 53°-13'-52" EAST, CONTINUING ALONG SAID SOUTHEASTERLY RIGHT-OF-WAY LINE, A DISTANCE OF 46.21 FEET TO THE POINT OF BEGINNING.

FROM THE POINT OF BEGINNING THUS DESCRIBED CONTINUE NORTH 53°-13'-52" EAST, ALONG THE AFOREMENNED SOUTHEASTERLY RIGHT-OF-WAY LINE, A DISTANCE OF 4.00 FEET TO A POINT; RUN THENCE NORTH 37°-07'-53" WEST, ALONG THE NORTHEASTERLY RIGHT-OF-WAY LINE, A DISTANCE OF 25.01 FEET TO A POINT; RUN THENCE IN A NORTHEASTERLY DIRECTION ALONG THE ARC OF A CURVE IN THE SOUTHEASTERLY RIGHT-OF-WAY LINE OF SAID HARRIETTS BLUFF ROAD, SAID CURVE BEING CONCAVE TO THE SOUTHEAST AND HAVING A RADIUS OF 1105.92 FEET, A CHORD DISTANCE OF 41.04 FEET TO A POINT, THE BEARING OF THE AFOREMENTIONED CHORD BEING NORTH 55°-28'-18" EAST; RUN THENCE SOUTH 37°-07'-53" EAST, A DISTANCE OF 35.00 FEET TO A POINT; RUN THENCE SOUTH 52°-52'-07" WEST, A DISTANCE OF 45.00 FEET TO A POINT; RUN THENCE NORTH 37°-07'-53" WEST, A DISTANCE OF 11.88 FEET TO THE POINT OF BEGINNING.

Attachment: Bluff Quit Claim (2128 : Approval Of: Quit Claim Deed)

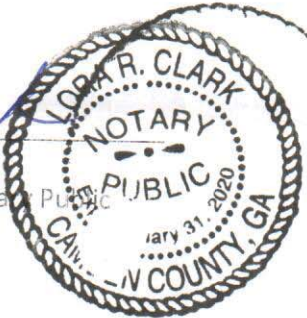
TO HAVE AND TO HOLD the said bargained premise to the said party of the second part, so that neither the said party of the first part nor its successors and assigns, not any other person or persons claiming under it shall at any time by any means or ways, have, claim or demand any right or title to the aforesaid described premises or appurtenances, or any rights thereof.

4/6/18
Date

Jeff Watson, mayor
S.W.S., L.L.C.

STATE OF GA, Blount COUNTY

Before me, the undersigned, a Notary Public in and for said County and State, this 6 day of April, 2018, personally appeared SWS, L.L.C., and acknowledged the execution of the foregoing Quit Claim Deed as his/her free and voluntary act and deed. In witness whereof, I have hereunto subscribed my name and affixed my official seal.

Lora Clark
Notary Public


CITY OF KINGSLAND

T. Thutcher
Witness

Kenneth E. Smith, Sr., Mayor

ATTEST:

Notary Public

Linda O'Shaughnessy, City

Packet Pg. 8

Attachment: Bluff Quit Claim (2128 : Approval Of: Quit Claim Deed)

**Criminal Justice
Man-Made/Natural Disaster Policy**

Subject:

Man-Made/Natural Disaster Policy for information derived from the Georgia Crime Information Center (GCIC) Criminal Justice Information System (CJIS) Network

Effective Date: 09/23/2015

Revised Date: 04/3/2018

Purpose:

The purpose of this policy is to establish guidelines in the event of a man-made or natural disaster to ensure that GCIC CJIS Network material, records and information obtained thereof are secure.

This policy applies to all agency employees, non-paid employees, and vendors/contractors with access, to include physical and logical access, to GCIC materials, records and information. This policy will establish guidelines for securing GCIC materials, records and information obtained thereof in the event of a man-made or natural disaster.

All employees, non-paid employees, and vendors/contractors are required to follow the policies, rules and procedures set forth by GCIC, GCIC Council Rules, CJIS Security Policy, and the laws of the State of Georgia.

In the event of a man-made or natural disaster, the agency head or designee and/or the Local Agency Security Officer (LASO) shall have the responsibility of ensuring that GCIC materials and records maintained by the agency are not in danger of being damaged or destroyed. In the event that the materials or records are not secure, or have been damaged or destroyed, the affected agency personnel shall make immediate notification to the agency head or designee and/or LASO to inform of the situation. If necessary, personnel shall be stationed in the area to secure GCIC materials and records. Affected areas include: Records, and Administrative Offices. The agency head, designee and/or LASO shall be responsible for taking necessary steps to ensure that all materials and records are secure on-site or that the materials and records are moved to another secure location.

Policy Title:	Media Protection Policy
Effective Date:	9/23/2015
Revision Date:	Every 2 years or as needed
Approval(s):	Chief Terry Smith, Captain William Carreira
LASO:	William Carreira
CSO:	
Agency Head:	Terry Smith

Purpose:

The intent of the Media Protection Policy is to ensure the protection of the Criminal Justice Information (CJI) until such time as the information is either released to the public via authorized dissemination (e.g. within a court system or when presented in crime reports data), or is purged or destroyed in accordance with applicable record retention rules.

This Media Protection Policy was developed using the FBI's Criminal Justice Information Services (CJIS) Security Policy 5.1 dated 7/13/2012. The *Kingsland Fire Rescue* may complement this policy with a local policy; however, the CJIS Security Policy shall always be the minimum standard. The local policy may augment, or increase the standards, but shall not detract from the CJIS Security Policy standards.

Scope:

The scope of this policy applies to any electronic or physical media containing FBI Criminal Justice Information (CJI) while being stored, accessed or physically moved from a secure location from the *Kingsland Fire Rescue*. This policy applies to any authorized person who accesses, stores, and / or transports electronic or physical media. Transporting CJI outside the agency's assigned physically secure area must be monitored and controlled.

Authorized *Kingsland Fire Rescue* personnel shall protect and control electronic and physical CJI while at rest and in transit. The *Kingsland Fire Rescue* will take appropriate safeguards for protecting CJI to limit potential mishandling or loss while being stored, accessed, or transported. Any inadvertent or inappropriate CJI disclosure and/or use will be reported to the *Kingsland Fire Rescue* Local Agency Security Officer (LASO). Procedures shall be defined for securely handling, transporting and storing media.

Media Storage and Access:

Controls shall be in place to protect electronic and physical media containing CJI while at rest, stored, or actively being accessed. "Electronic media" includes memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, backup medium, optical disk, flash drives, external hard drives, or digital memory card. "Physical media" includes printed documents and imagery that contain CJI.

To protect CJI, the *Kingsland Fire Rescue* personnel shall:

1. Securely store electronic and physical media within a physically secure or controlled area. A secured area includes a locked drawer, cabinet, or room.
2. Restrict access to electronic and physical media to authorized individuals.
3. Ensure that only authorized users remove printed form or digital media from the CJI.
4. Physically protect CJI until media end of life. End of life CJI is destroyed or sanitized using approved equipment, techniques and procedures. (See Sanitization Destruction Policy)
5. Not use personally owned information system to access, process, store, or transmit CJI unless the *Kingsland Fire Rescue* has established and documented the specific terms and conditions for personally owned information system usage. (See Personally Owned Device Policy)
6. Not utilize publicly accessible computers to access, process, store, or transmit CJI. Publicly accessible computers include but are not limited to: hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.
7. Store all hardcopy CJI printouts maintained by the *Kingsland Fire Rescue* in a secure area accessible to only those employees whose job function require them to handle such documents.
8. Safeguard all CJI by the *Kingsland Fire Rescue* against possible misuse by complying with the Physical Protection Policy, Personally Owned Device Policy, and Disciplinary Policy.
9. Take appropriate action when in possession of CJI while not in a secure area:
 - a. CJI must not leave the employee's immediate control. CJI printouts cannot be left unsupervised while physical controls are not in place.
 - b. Precautions must be taken to obscure CJI from public view, such as by means of an opaque file folder or envelope for hard copy printouts. For electronic devices like laptops, use session lock use and /or privacy screens. CJI shall not be left in plain public view. When CJI is electronically transmitted outside the

boundary of the physically secure location, the data shall be immediately protected using encryption.

- i. When CJI is at rest (i.e. stored electronically) outside the boundary of the physically secure location, the data shall be protected using encryption. Storage devices include external hard drives from computers, printers and copiers used with CJI. In addition, storage devices include thumb drives, flash drives, back-up tapes, mobile devices, laptops, etc.
 - ii. When encryption is employed, the cryptographic module used shall be certified to meet FIPS 140-2 standards.
10. Lock or log off computer when not in immediate vicinity of work area to protect CJI. Not all personnel have same CJI access permissions and need to keep CJI protected on a need-to-know basis.
11. Establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of CJI. (See Physical Protection Policy)

Media Transport:

Controls shall be in place to protect electronic and physical media containing CJI while in transport (physically moved from one location to another) to prevent inadvertent or inappropriate disclosure and use. "Electronic media" means electronic storage media including memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, backup medium, optical disk, flash drives, external hard drives, or digital memory card.

Dissemination to another agency is authorized if:

1. The other agency is an Authorized Recipient of such information and is being serviced by the accessing agency, or
2. The other agency is performing personnel and appointment functions for criminal justice employment applicants.

The *Kingsland Fire Rescue* personnel shall:

1. Protect and control electronic and physical media during transport outside of controlled areas.
2. Restrict the pickup, receipt, transfer and delivery of such media to authorized personnel.

The *Kingsland Fire Rescue* personnel will control, protect, and secure electronic and physical media during transport from public disclosure by:

1. Use of privacy statements in electronic and paper documents.
2. Limiting the collection, disclosure, sharing and use of CJI.
3. Following the least privilege and role based rules for allowing access. Limit access to CJI to only those people or roles that require access.
4. Securing hand carried confidential electronic and paper documents by:
 - a. Storing CJI in a locked briefcase or lockbox.
 - b. Only viewing or accessing the CJI electronically or document printouts in a physically secure location by authorized personnel.
 - c. For hard copy printouts or CJI documents:
 - i. Package hard copy printouts in such a way as to not have any CJI information viewable.
 - ii. That are mailed or shipped, agency must document procedures and only release to authorized individuals. DO NOT MARK THE PACKAGE TO BE MAILED CONFIDENTIAL. Packages containing CJI material are to be sent by method(s) that provide for complete shipment tracking and history, and signature confirmation of delivery. (Agency Discretion)
5. Not taking CJI home or when traveling unless authorized by *Kingsland Fire Rescue* LASO. When disposing confidential documents, use a shredder.

Electronic Media Sanitization and Disposal:

The agency shall sanitize, that is, overwrite at least three times or degauss electronic media prior to disposal or release for reuse by unauthorized individuals. Inoperable electronic media shall be destroyed (cut up, shredded, etc.). The agency shall maintain written documentation of the steps taken to sanitize or destroy electronic media. Agencies shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel. Physical media shall be securely disposed of when no longer required, using formal procedures. For end of life media policy, refer to "Sanitization Destruction Policy".

Breach Notification and Incident Reporting:

The agency shall promptly report incident information to appropriate authorities. Information security events and weaknesses associated with information systems shall be communicated in a manner allowing timely corrective action to be taken. Incident related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports.

Roles and Responsibilities:

If CJI is improperly disclosed, lost, or reported as not received, the following procedures must be immediately followed:

1. *Kingsland Fire Rescue* personnel shall notify his/her supervisor or LASO, and an incident-report form must be completed and submitted within 24 hours of discovery of the incident. The submitted report is to contain a detailed account of the incident, events leading to the incident, and steps taken/to be taken in response to the incident. (Agency Discretion)
2. The supervisor will communicate the situation to the LASO to notify of the loss or disclosure of CJI records.
3. The LASO will ensure the CSA ISO (CJIS System Agency Information Security Officer) is promptly informed of security incidents.
4. The CSA ISO will:
 - a. Establish a security incident response and reporting procedure to discover, investigate, document, and report to the CSA, the affected criminal justice agency, and the FBI CJIS Division ISO major incidents that significantly endanger the security or integrity of CJI.
 - b. Collect and disseminate all incident-related information received from the Department of Justice (DOJ), FBI CJIS Division, and other entities to the appropriate local law enforcement POCs within their area.
 - c. Act as a single POC for their jurisdictional area for requesting incident response assistance.

Penalties:

Violation of any of the requirements in this policy by any authorized personnel will result in suitable disciplinary action, up to and including loss of access privileges, civil and criminal prosecution and / or termination.

Acknowledgement:

I have read the policy and rules above and I will:

- Abide by the *Kingsland Fire Rescue's* Media Protection Policy. I understand any violation of this policy may result in discipline up to and including termination.
- Report any *Kingsland Fire Rescue* CJI security incident to Supervisor and / or LASO as identified in this policy.

Signature: _____ Date: _____/____/____

Questions

Any questions related to this policy may be directed to the *Kingsland Fire Rescue's* LASO:

LASO Name:	LASO Phone:	LASO email:
State C/ISO Name:	C/ISO Phone:	C/ISO email:

Other Related Policy Reference:

- See Media Sanitization and Destruction Policy
- Media Disposal Policy
- Physical Protection Policy

KINGSLAND FIRE RESCUE
DISCIPLINARY POLICY

DISCIPLINARY POLICY

In support of Kingsland Fire Rescue's mission of public service to the City of Kingsland/ Camden County citizens, the Kingsland Fire Rescue provides the needed technological resources needed to personnel to access FBI CJIS systems and information in support of the agency's mission. All agency personnel, with access to FBI Criminal Justice Information (CJI) or any system with stored FBI CJI, have a duty to protect the system and related systems from physical and environmental damage and are responsible for correct use, operation, care and maintenance of the information. All technology equipment: computers, laptops, software, copiers, printers, terminals, MDTs, mobile devices, live scan devices, fingerprint scanners, software to include RMS/CAD, operating systems, etc., used to process, store, and/or transmit FBI CJIS is a privilege allowed by Kingsland Fire Rescue, state CSO, and the FBI. To maintain the integrity and security of the Kingsland Fire Rescue's and FBI's CJIS systems and data, this computer use privilege requires adherence of relevant federal, state and local laws, regulations and contractual obligations. All existing laws and Kingsland Fire Rescue regulations and policies apply, including not only those laws and regulations that are specific to computers and networks, but also those that may apply to personal conduct.

Misuse of computing, networking or information resources may result in temporary or permanent restriction of computing privileges up to employment termination. In some misuse situations, account privileges will be suspended to prevent ongoing misuse while under investigation. Additionally, misuse can be prosecuted under applicable statutes. All files are subject for search. Where follow-up actions against a person or agency after an information security incident involves legal action (either civil or criminal), the evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s). Complaints alleging misuse of Kingsland Fire Rescue's computing and network resources and FBI CJIS systems and/or data will be directed to those responsible for taking appropriate disciplinary action.

Examples of Misuse with access to FBI CJI

1. Using someone else's login that you are not the owner.
2. Leaving computer logged in with your login credentials unlocked in a physically unsecure location allowing anyone to access Kingsland Fire Rescue systems and/or FBI CJIS systems and data in your name.
3. Allowing unauthorized person to access FBI CJI at any time for any reason. Note: Unauthorized use of the FBI CJIS systems is prohibited and may be subject to criminal and/or civil penalties.
4. Allowing remote access of Kingsland Fire Rescue issued computer equipment to FBI CJIS systems and/or data without prior authorization by Kingsland Fire Rescue.
5. Obtaining a computer account that you are not authorized to use.
6. Obtaining a password for a computer account of another account owner.
7. Using the Kingsland Fire Rescue's network to gain unauthorized access to FBI CJI.

KINGSLAND FIRE RESCUE
DISCIPLINARY POLICY

8. Knowingly performing an act which will interfere with the normal operation of FBI CJIS systems.
9. Knowingly propagating a computer virus, Trojan horse, worm and malware to circumvent data protection or compromising existing security holes to FBI CJIS systems.
10. Violating terms of software and / or operating system licensing agreements or copyright laws.
11. Duplication of licensed software, except for backup and archival purposes that circumvent copyright laws for use in Kingsland Fire Rescue, for home use or for any customer or contractor.
12. Deliberately wasting computing resources to include streaming audio, videos for personal use that interferes with Kingsland Fire Rescue network performance.
13. Using electronic mail or instant messaging to harass others.
14. Masking the identity of an account or machine.
15. Posting materials publicly that violate existing laws or Kingsland Fire Rescue's codes of conduct.
16. Attempting to monitor or tamper with another user's electronic mail or files by reading, copying, changing, or deleting without explicit agreement of the owner.
17. Using *Kingsland Fire Rescue's* technology resources to advance unwelcome solicitation of a personal or sexual relationship while on duty or through the use of official capacity.
18. Unauthorized possession of, loss of, or damage to *Kingsland Fire Rescue's* technology equipment with access to FBI CJI through unreasonable carelessness or maliciousness.
19. Maintaining FBI CJI or duplicate copies of official *Kingsland Fire Rescue's* files in either manual or electronic formats at his or her place of residence or in other physically non-secure locations without express permission.
20. Using *Kingsland Fire Rescue's* technology resources and/or FBI CJIS systems for personal or financial gain.
21. Deliberately failing to report promptly any known technology-related misuse by another employee that may result in criminal prosecution or discipline under this policy.
22. Using personally owned devices on *Kingsland Fire Rescue's* network to include personally-owned thumb drives, CDs, mobile devices, tablets on Wi-Fi, etc. Personally owned devices should not store *Kingsland Fire Rescue's* data, State data, or FBI CJI.

The above listing is not all-inclusive and any suspected technology resource or FBI CJIS system or FBI CJI misuse will be handled by Kingsland Fire Rescue's on a case by case basis. Activities will not be considered misuse when authorized by appropriate Kingsland Fire Rescue's officials for security or performance testing.

KINGSLAND FIRE RESCUE DISCIPLINARY POLICY

Privacy Policy

All agency personnel utilizing agency-issued technology resources funded by *Kingsland Fire Rescue's* expressly acknowledges and agrees that such service, whether for business or personal use, shall remove any expectation of privacy. Use of *Kingsland Fire Rescue's* systems indicates consent to monitoring and recording.

The *Kingsland Fire Rescue's* reserves the right to access and audit any and all communications including electronic and physical media at rest, in transit and at end of life. *Kingsland Fire Rescue's* personnel shall not store personal information with an expectation of personal privacy that are under the control and management of *Kingsland Fire Rescue's*.

Personal Use of Agency Technology

The computers, electronic media and services provided by *Kingsland Fire Rescues* are primarily for business use to assist personnel in the performance of their jobs. Limited, occasional, or incidental use of electronic media (sending or receiving) for personal, non-business purposes is understandable and acceptable, and all such use should be done in a manner that does not negatively affect the systems' use for their business purposes.

However, employees are expected to demonstrate a sense of responsibility and not abuse this privilege.

Misuse Notification

Due to the increase in the number of accidental or malicious computer attacks against both government and private agencies, *Kingsland Fire Rescue's* shall: (i) establish an operational incident handling capability for all information systems with access to FBI CJIS systems and data. This includes adequate preparation, detection, analysis, containment, recovery, and user response activities; (ii) track, document, and report incidents to appropriate agency officials and/or authorities.

ISOs have been identified as the POC on security-related issues for their respective agencies and shall ensure LASOs institute the CSA incident response reporting procedures at the local level.

All *Kingsland Fire Rescue's* personnel are responsible to report misuse of *Kingsland Fire Rescue's* technology resources to appropriate *Kingsland Fire Rescue's* officials.

Local contact-LASO: bcarreira@kingslandga.gov Phone: 912-729-8280

Contact-CSA ISO: [firstnamelast@state.gov](mailto:firstname.lastname@state.gov) Phone: _____

I have read the policy and rules above and I will abide in the *Kingsland Fire Rescue's* Disciplinary policy.

Signature: _____ Date: _____/_____/_____

Disposal of Media Policy and Procedures

1.0 Purpose

The purpose of this policy is to outline the proper disposal of media (physical or electronic) at *Kingsland Fire Rescue*. These rules are in place to protect sensitive and classified information, employees and *Kingsland Fire Rescue*. Inappropriate disposal of *Kingsland Fire Rescue* and FBI Criminal Justice Information (CJI) and media may put employees, *Kingsland Fire Rescue* and the FBI at risk.

2.0 Scope

This policy applies to all *Kingsland Fire Rescue* employees, contractors, temporary staff, and other workers at *Kingsland Fire Rescue* with access to FBI CJIS systems and/or data, sensitive and classified data, and media. This policy applies to all equipment that processes, stores, and/or transmits FBI CJI and classified and sensitive data that is owned or leased by *Kingsland Fire Rescue*

3.0 Policy

When no longer usable, hard drives, diskettes, tape cartridges, CDs, ribbons, hard copies, print-outs, and other similar items used to process, store and/or transmit FBI CJI and classified and sensitive data shall be properly disposed of in accordance with measures established by *Kingsland Fire Rescue*.

Physical media (print-outs and other physical media) shall be disposed of by one of the following methods:

- 1) Shredding using *Kingsland Fire Rescue* issued shredders.
- 2) Placed in locked shredding bins for [private contractor name] to come on-site and shred, witnessed by *Kingsland Fire Rescue* personnel throughout the entire process.
- 3) Incineration using *Kingsland Fire Rescue* incinerators or witnessed by *Kingsland Fire Rescue* personnel onsite at agency or at contractor incineration site, if conducted by non-authorized personnel.

Electronic media (hard-drives, tape cartridge, CDs, printer ribbons, flash drives, printer and copier Hard-drives, etc.) shall be disposed of by one of the <Agency Name> methods:

- 1) **Overwriting (at least 3 times)** - an effective method of clearing data from magnetic media. As the name implies, overwriting uses a program to write (1s, 0s, or a combination of both) onto the location of the media where the file to be sanitized is located.
- 2) **Degaussing** - a method to magnetically erase data from magnetic media. Two types of degaussing exist: strong magnets and electric degausses. Note that common magnets (e.g., those used to hang a picture on a wall) are fairly weak and cannot effectively degauss magnetic media.
- 3) **Destruction** – a method of destroying magnetic media. As the name implies, destruction of magnetic media is to physically dismantle by methods of crushing, disassembling, etc., ensuring that the platters have been physically destroyed so that no data can be pulled.

IT systems that have been used to process, store, or transmit FBI CJI and/or sensitive and classified information shall not be released from *Kingsland Fire Rescue's* control until the equipment has been sanitized and all stored information has been cleared using one of the above methods.

4.0 Enforcement

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