LInX

610.1 PURPOSE

The National Capital Region Law Enforcement Information Exchange (LInX) is a collaborative effort between the Metropolitan Washington Council of Governments and the Naval Criminal Investigative Service. LInX is designed to allow authorized users access to law enforcement information provided by participating agencies via a central depository. LInX integrates electronically available law enforcement data from participating agencies records systems and provides users with advanced query and analytical tools to assist with criminal investigations, development of crime prevention and enforcement strategies. The St. Mary's County Sheriff's Office through agreement with the National Capitol Region LInX Governance Board is a participating agency.

610.2 GENERAL LINX SYSTEM USAGE

The LInX System Administrator, designated by the Sheriff, is responsible for the agency's management and operations of the LInX Program to include training. The system administrator will maintain a file containing a list of qualified LInX Trainers, authorized users to include a record of training, and the originals of the signed LInX user agreements.

The St. Mary's County Government Information Technology Department (IT) will be responsible for the daily administration of the LInX connection and data upload.

Access to the LInX System is restricted to all sworn officers and analysts of the Patrol Division as well as members of the Criminal Investigations Division, Vice/Narcotics Division, Administration Division, Special Operations Division, Human Resources and Child Support Enforcement. Before being granted access to the system, employees are required to review the LInX Operational Policy and Rules, sign a LInX user agreement and receive training from an authorized trainer on the proper use of the system.

LInX users are required to receive one (1) hour of training every two (2) years to maintain their system access. This training may be accomplished by attending a LInX sponsored training or reviewing training videos made available via the training tab on the LInX homepage.

It is the responsibility of each authorized user to ensure this technology is only used for conducting authorized agency business as outlined within the National Capital Region Law Enforcement Information Exchange Operational Policy and Rules.

610.3 SYSTEM SECURITY

It is the authorized users' responsibility to ensure the security of the LInX System against unauthorized use.

(a) Password – Password to access the LInX system will not be shared or made known to any other individual, nor will the authorized user leave their password in any discernible written form in or near their computer. Personnel will be held strictly accountable for any transactions appearing under their log on signature and password. Personnel

who have reason to believe their password has been compromised will immediately notify the system administrator and change their password utilizing the procedures outlined during LInX training. An attempt by any employee to utilize LInX with another employee's password is strictly prohibited.

(b) Security Administrator – The Information Systems and Analytics Manager or designee will serve as the LInX Security Administrator. They will make periodic checks of the electronic user activity logs to ensure the system is being used in accordance with agency policy and the National Capital Region Law Enforcement Information Exchange Operational Policy and Rules. An annual audit will be conducted by the Security Administrator in accordance with the audit guidelines set forth by the National Capital Region LInX Governance Board. The results of the audit will be forwarded to the Assistant Sheriff/Sheriff via detailed report each year.

610.4 TERMINATION OF ACCESS

(a) The Security Administrator shall terminate access upon any of the following conditions:

1. The user is no longer employed by the Agency.
2. The user no longer has a legitimate purpose to have access to LInX.
3. The user is no longer in good standing.