LInX Northwest Program

814.1 PURPOSE AND SCOPE

This policy clarifies the Law Enforcement Information Exchange (LInX) Northwest system requirements to include but not limited to, physical security of the LInX program, LInX information and the requirement to use and disseminate the shared information.

814.2 POLICY

The LInX system is a law enforcement information sharing partnership involving local, state, and federal law enforcement agencies in the Pacific Northwest. LInX has been developed to improve public safety, solve crimes, and prevent terrorism. LInX is a partnership built on trust and to maintain the trust following the rules are upheld by all LInX agencies. Violations of this policy may results in sanctions against an individual user or Regional Partner Agency (RPA).

814.3 DEPARTMENT RESPONSIBILITIES

Each RPA shall contribute information to LInX Northwest, once a connection is made, and agrees to permit the access, dissemination, and/or use of such information by every other partner agency in LInX Northwest. The contributing party has sole responsibility and accountability for ensuring this it is not constrained from permitting this by any laws, regulations, policies, and procedures applicable to the submitting party.

The Department LInX Administrator will conduct an annual audit to assure compliance with LInX Northwest system requirements.

814.3.1 INFORMATION ACCESSIBILTY AND SECURITY

Information obtained through LInX Northwest is considered Criminal Justice Information System (CJIS) information and shall be treated with the same security measures outlined in the Protected Information and ACCESS Policies. In addition to those measures, the following measures which are unique to LInX Northwest protocol shall be adhered to:

(a) A user may only access LInX when he/she has a legitimate, official law enforcement purpose after receiving LInX training.

(b) Information in the system shall not be disseminated outside of an accessing party without first obtaining express permission of each party that contributed the information in question. LInX users who wish to use information in LInX for the preparation of judicial process (e.g., affidavits, warrants, or subpoenas) agree to not print and use information from LInX, but to contact the originating agency who will provide a copy of the original report to the requestor for court or other official uses.

(c) Printing copies from LInX is highly restricted. Users may only retain printed copies temporarily and shall not place copies in an official file or submit them to a court. Printed copies must be destroyed or shredded. Printed copies may not be made for members of non-participating agencies.

(d) Any requests for reports or data in LInX records from anyone other than an RPA to this exhibit will be directed to the contributing agency. Participating agencies in LInX agree to not disclose another agency's reports or information to a third party. Even when an agency receives an official request for disclosure, LInX agencies agree to refer such requests to the originating agency of the report for action.

(e) Only pertinent information, obtained through LInX, used in the furtherance of an investigation should be listed in the report. Irrelevant and non-essential information should not be documented or listed as an investigatory resource.

(f) Each agency retains sole ownership of, sole responsibility for, and exclusive control over the content of the information that it contributes to LInX, and it may, at will, at any time update, correct or delete the information that it contributes to LInX.

814.4   SECURITY MEASURES

The Vancouver Police Department has adopted the following security measures to comply with applicable laws and regulations and to prevent unauthorized access to the LInX system and its data.

814.4.1   SYSTEM SECURITY

A Regional Partner Agency will have access to LInX via a secure internet connection. It is the RPA's responsibility to provide and maintain their own internet connectivity to LInX.

Department personnel can only utilize the LInX system to obtain CJIS information from secure terminal from a secure location. A secure terminal is any Department owned or approved electronic device, mobile data terminal (MDT), desk top computer, laptop or wireless device. A secure location is considered to be inside any Vancouver Police building or police vehicle.

Accessing LInX from any other device or location is prohibited.

LInX will maintain an audit capability that will log the date, time, subject, and originating account of all user queries. The LInX Governance Board will maintain these audit logs for at least five years.

The Department LInX Administrator has the authority to immediately disable an officer's LInX account who violates the LInX policy, is under criminal investigation, retires, resigns, is terminated or leaves the Agency for any reason.

814.5   TRAINING

Only officers who are ACCESS certified and have received the approved LInX training will be granted authorization to access LInX Northwest. Any updated training will be coordinated though the designated Vancouver Police Department LInX Administrators.