TRANSIT POLICE

AUTOMATED CRIMINAL INTELLIGENCE INFORMATION SYSTEM (ACIIS)

Effective Date: December 16, 2011
Revised Date:
Reviewed Date:
Review Frequency: As Required
Office of Primary Responsibility: Deputy Chief Officer Operations

POLICY

Definitions

ACIIS (and ACIIS system) – The Automated Criminal Intelligence Information System, a National Police Service administered by CISC. ACIIS is the Canadian law enforcement community's national database for criminal information and intelligence on organized and Serious Crime. FIPPA s.15 - Harm to Law Enforcement

Authorized User – A Transit Police staff person granted the privilege of access to the ACIIS system.

Chief Officer – The Transit Police Chief Officer or delegate.

CISC – The Criminal Intelligence Service Canada.

CISC Category I Police Agency – The agency has full police officer authority provided under a Canadian federal or provincial police act. The primary role of the agency is law enforcement and the agency contributes to the criminal intelligence process.

CISBC/YT – The CISC Provincial Bureau in British Columbia.

Contributing Member Agency – Under the direction of the Commissioner, Chief of Police, Director or equivalent a contributing member agency will be responsible for: meaningful participation; and contribution and maintenance of accurate, pertinent data in the ACIIS database. The Transit Police is a Contributing Member Agency in CISC.

Designated Constables – The Transit Police police officers appointed by the Police Board.

Member – A Transit Police Designated Constable, the Chief Officer or a Deputy Chief Officer of the Transit Police.

NPSNet – The National Police Services Network.

Organized Crime – Organized crime or criminal organization as defined in the Criminal Code of Canada, means a group, however organized, that:

a. is composed of three or more persons in or outside Canada; and
b. has as one of its main purposes or main activities the facilitation or commission of one or more serious offences that, if committed, would likely result in the direct or indirect receipt of a material benefit, including a financial benefit, by the group or by any of the persons who constitute the group.
c. It does not include a group of persons that forms randomly for the immediate commission of a single offence.

PRIME – The Police Records Information Management Environment used by police agencies in British Columbia, including the Transit Police.

Restricted Record – A restricted record is FIPPA s.15 - Harm to Law Enforcement

Serious Crime – Serious offence or crime as defined in the Criminal Code of Canada, means an indictable offence under this or any other Act of Parliament for which the maximum punishment is imprisonment for five (5) years or more, or another offence that is prescribed by regulation.

Third Party Rule – The Third Party Rule means that the information must not be used, copied, reproduced, or further disseminated without the consent of the originator.

Transit Police – The South Coast British Columbia Transportation Authority Police Service.

Unrestricted Record – A record which is entered on the system by the maintenance unit of an agency and is available to all ACIIS users.

Authority

1. The CISC Constitution and Regulations mandates the sharing of criminal intelligence among Canadian enforcement agencies in Canada and establishes guidelines governing the use of ACIIS by CISC member agencies.

2. The Transit Police, as a CISC Category 1 Police Agency, is permitted to have direct full time access to the ACIIS system and network. The conditions of direct full time access are as described in the CISC Constitution and Regulations, CISC ACIIS Policy and Regulations, and related Memoranda of Understanding.

3. CISC, in coordination with the RCMP Chief Information Officer Sector, will establish the speed/bandwidth and appropriate network security measures necessary to meet the Transit Police access needs.

General

4. The Transit Police access to the ACIIS system will be for law enforcement functions/purposes only and, in accordance with ACIIS policy and the Transit Police legal mandate.

5. The Transit Police will use the ACIIS system in the manner required by the managing body and by Transit Police policy and procedures. The ACIIS system will be not utilized for any purpose other than its mandated use.

6. The Transit Police understands that, in accordance with the CISC Constitution and Regulations, all information that the Transit Police enters into ACIIS or supplies to ACIIS, unless the record is restricted, will be made available to all CISC Category 1 member agencies whether the agencies have direct access to ACIIS or not. ACIIS data integrity is the responsibility of the Contributing Member Agency.

7. All Authorized Users to ACIIS will be required to review the ACIIS Policy prior to use of the system.

8. The Transit Police will ensure that ACIIS is only used within the Transit Police office space approved by CISC as per the site security application.

9. The Transit Police will ensure that all personnel having terminal access to the ACIIS system are security screened in accordance to the CISC Constitution and Regulations, ACIIS Policy and Regulations, and related Memoranda of Understanding. Proof of the security screening will be kept and made available, upon request, to CISC auditors and the CISBC/YT ACIIS Coordinator.

    1. Pursuant to the ACIIS Policy, all personnel granted ACIIS access are required to have an RCMP Reliability Status or equivalent security clearance, and all accredited personnel employed by a recognized Category 1 Police Agency are considered to hold the status equivalent to an RCMP Reliability Status.

    2. The Memorandum of Understanding with CISBC/YT requires Transit Police personnel who will have access to ACIIS to have a criminal record check through the submission of fingerprints to the Directorate of Information and Identification Services of the RCMP, prior to being permitted access to ACIIS.

10. Before an Authorized User is given access to an ACIIS terminal, the Authorized User will receive appropriate training from ACIIS trainers or from qualified personnel within the Transit Police.

11. The Transit Police will implement strict measures to prevent network or computer security breaches which may result in the disclosure, the modification or the deletion of information obtained from or residing in the ACIIS system.

12. The Transit Police will assume responsibility for all access to the ACIIS system from any device located on the Transit Police side of the network connection or interface.

13. The Transit Police acknowledges the necessity to respect the privacy of individuals and to protect the data available through the ACIIS system. The Transit Police will comply with applicable provincial or federal access to information and privacy laws.

14. The Transit Police will not disseminate any information obtained from the ACIIS Data Bank, except where that use is consistent with the ACIIS Policy. The Transit Police may however disseminate ACIIS information to another approved ACIIS agency provided it does not conflict with provincial or federal privacy legislation and a Letter of Understanding is in place between the agencies concerned.

ACIIS Policy and Security Violations

15. The Transit Police will report all complaints of ACIIS policy and security violations to CISC, through CISBC/YT. The Transit Police or agencies involved will investigate thoroughly and expediently all complaints of ACIIS policy violations. The results of the investigation, including corrective or disciplinary action that has been taken, will be reported to the Director General of CISC and the CISBC/YT.

16. If complaints of ACIIS policy and security violations cannot, for whatever reason, be resolved by the Transit Police, the Transit Police acknowledges that the Director General of CISC will have an investigation conducted by the Deputy Director General of ACIIS.

17. The Transit Police will report any and all known or suspected breaches of security or misuse of the system, and send the details of the breach and the result of the investigation to the appropriate ACIIS Manager.

ACIIS Liaison

18. The Chief Officer will appoint an ACIIS Liaison Officer.

PROCEDURES

Access

19. The Transit Police computers that have ACIIS system access must be installed and maintained in locations that have been pre-approved by CISBC/YT.

20. FIPPA s.15 - Harm to Law Enforcement

21. ACIIS access privileges will be granted FIPPA s.15 - Harm to Law Enforcement

***NOTE**: CISC shall directly, or through the CISBC/YT, set the standards for the ACIIS training course and supply to the Transit Police any training material and reference material required to comply with the training requirements as stipulated in the ACIIS Policy.*

22. Each Authorized User will be provided with FIPPA s.15 - Harm to Law Enforcement .

23. Each Authorized User will be responsible for any transaction undertaken in the ACIIS system under their access privilege and any misuse of access privileges will be dealt with by way of the Transit Police disciplinary policies.

24. No Transit Police device that has access to the ACIIS system will FIPPA s.15 - Harm to Law Enforcement

ACIIS File Entry Criteria

25. The Transit Police will add intelligence/information to the ACIIS system that conforms to the national, regional, provincial or local priorities.

26. FIPPA s.15 - Harm to Law Enforcement

ACIIS File Guideline

27. FIPPA s.15 - Harm to Law Enforcement

28. For the purposes of clarification, FIPPA s.15 - Harm to Law Enforcement

29. In addition FIPPA s.15 - Harm to Law Enforcement

30. The following may be FIPPA s.15 - Harm to Law Enforcement

31. Information added by the Transit Police to ACIIS which originated from another agency will be verified for reliability with, and have the consent of, the originating agency.

Restricted Records

32. The ACIIS Restricted Record category is FIPPA s.15 - Harm to Law Enforcement

33. Files entered in the ACIIS database in the Restricted Record Category must have the written approval of the Transit Police Chief Officer or designate.

34. FIPPA s.15 - Harm to Law Enforcement

    Exceptional Circumstances: FIPPA s.15 - Harm to Law Enforcement

35. All documents added as Restricted Records to ACIIS will be written so they may be shared without further vetting when the file may be unrestricted.

36. Restricted ACIIS entries will FIPPA s.15 - Harm to Law Enforcement

Maintenance of Records

37. ACIIS is designed to be a paperless system and is solely an intelligence data bank. The responsibility for maintaining ACIIS records will be with the Transit Police Intel Section.

38. All records entered by the Transit Police Authorized Users into ACIIS will:

    1. correspond to an existing Transit Police General Occurrence (GO) file number on the PRIME (the number will be noted in the comment text field of all entries or in the File Reference section of ACIIS);
    2. include the name of the person responsible for the record;
    3. include a diary date for review of the file;
    4. not include a review diary date to exceed 10 years from the previous review diary date;
    5. be maintained, applied, and used in accordance with the Transit Police record keeping and review policy;
    6. have support documentation for the ACIIS file (may be in either electronic or paper format).

39. ACIIS Policy requires that information that can no longer be validated must be immediately purged from the ACIIS database. Removal of records from the ACIIS database will be based on the Transit Police records management policies.

40. In accordance with the ACIIS Memorandum of Understanding, the Transit Police will allow, when deemed necessary, the duplication and the sharing of its PRIME records by adding them to ACIIS as supporting documentation for ACIIS entries. All information shall be identical to the original file with no modifications in order to preserve the integrity of the document.

41. Any Transit Police reports or bulletins sent to CISBC/YT will be entered into the ACIIS database.

Release and Dissemination of Information

42. The originator/contributor of the criminal intelligence/information in ACIIS has the sole responsibility for document protection, designation, classification and will clearly indicate the designation, classification desired in accordance with the procedures listed in the CISC Constitution and Regulations.

43. The Transit Police will respect the privacy of individuals and comply with the provisions of the Privacy Act, Access to Information Act, Provincial Data Protection Legislation, and the Federal Treasury Board Guidelines as they may apply.

44. When dealing with ACIIS files, “Third Party Rule” applies and thus no information will be disseminated without the consent of the owner of the information.

45. The Transit Police will promptly notify the originating agency of any request for disclosure. This will include the nature of any order or request and the content of information to be disclosed, prior to any disclosure of the information. The final decision to share information will always rest with the originating agency.

46. ACIIS is an intelligence data bank only. No information obtained from ACIIS can be used for court purposes or to obtain a search warrant.

Audits

47. The Transit Police will permit CISC auditors and the CISBC/YT ACIIS Coordinator access to the Transit Police facilities for the purpose of auditing the Transit Police use of the ACIIS system and network(s) on which it operates to ensure compliance with the terms of the Memorandum of Understanding, ACIIS Policy, and the use and dissemination of information from the ACIIS system. This permission includes access to any computer terminal accessing the ACIIS system, terminal operators and relevant ACIIS documentation.

48. The Transit Police will provide CISC auditors with all applicable documentation to confirm the validity for entering records on the ACIIS system and will render all necessary assistance to CISC auditors to enable a complete physical audit of the Transit Police's ACIIS operations.

49. The Transit Police will remove or correct, at the request of an auditor, a record entry that does not conform to the ACIIS Policy.

Physical and Information Technology Security

50. The Transit Police will submit to the Director General of CISC, a completed NPSNet Connection Authorization/Change Request form and a system diagram describing the agency's technical environment. CISC must be informed of all proposed changes to the Transit Police technical environment for consideration of their technical and security impact on the ACIIS system, the NPSNet and the Transit Police, in accordance with the ACIIS Policy.

51. The Transit Police will be responsible for its own security of the ACIIS system and records. This security must meet or exceed the Canadian Police Information Centre (CPIC) security standards as outlined in the CPIC Reference Manual.

52. The Transit Police will keep CISC and CISBC/YT ACIIS system documentation and supplied software secure and ensure that it is not copied or duplicated in any form or distributed to anyone other than the intended agency, without the prior written approval of CISBC/YT.

53. All printed ACIIS documents must be shredded or burned.

54. All Transit Police ACIIS terminals must be serviced by persons authorized by the CISC.

Key References

Canadian Intelligence Service Canada (CISC) – ACIIS Policy [August 2010]
Canadian Intelligence Service Canada (CISC) – Regulations: Addendum to ACIIS Policy [August 2009]
Canadian Intelligence Service Canada (CISC) – Constitution [August 2006]
Canadian Intelligence Service Canada (CISC) – Regulations [August 2006]
Memorandum of Understanding between the Transit Police and CISC [October 2011]
Memorandum of Understanding between the Transit Police and CISBC/YT [October 2011]