TRANSIT POLICE

IT ACCESS CONTROL

Effective Date: August 8, 2012, October 24, 2023
Revised Date:
Reviewed Dated:
Review Frequency: Three Years
Office of Primary Responsibility: Inspector Administrative Support Management

POLICY

Definitions

Access Accounts – Information Technology (IT) defines generic, resource, system and User access accounts as follows:

A) Generic Account – A User account that is available and used by multiple Users to actively log on to an application, system or device. Generic User accounts are not permitted. All Users must have their own login accounts for accessing applications, devices and systems.

B) Resource Account – Accounts set up so that Users can use a specific functionality via indirect methods but is not used by any User as an active login to an application, system or device [redacted]

C) System Account – Accounts that are required to provide system, application, script authentication rights or privileges to execute properly. Such accounts are not used by any User for direct login [redacted]

D) User Account – An account provided to each individual User for logging into an application, device or system to perform tasks [redacted]

Business Owner – The specific Transit Police Personnel assigned by their Manager as the Office of Primary Interest ("OPI") for each App/Program at the Transit Police. Typically, this is the Transit Police Manager with primary use/responsibility for the App/Program output, and who will represent the business interests for the App/Program in terms of licensing, renewals, changes to the access controls, including access approvals [redacted]

Business Specific Apps/Programs – The Apps/Programs that are not part of the Core Apps/Programs [redacted]

Chief Officer – The Transit Police Chief Officer or delegate.

Core Apps – The Apps/Programs that are common to all Transit Police Personnel regardless of position [redacted]

Deputy Chief Officer Administrative Services – The Transit Police Deputy Chief Officer in charge of the Administrative Services Division or delegate.

FOIPPA – The *BC Freedom of Information and Protection of Privacy Act*, RSBC 1996, c.165, as amended from time to time.

Metro Vancouver Transit Police ("Transit Police") – The operating name of the South Coast British Columbia Transportation Authority Police Service (Designated Policing Unit and Designated Law Enforcement Unit).

Mobile Computing Device – A portable computer, mobile phone or other electronic information storage device.

Multi-Factor Authentication – Transit Police has adopted a Two Factor Authentication (2FA) technical system Section 15 FOIPPA - Disclosure harmful to law enforcement to authorize access at the network layer, where a trusted identity and two different authentication factors are used. Using two authentication factors, as opposed to one, delivers a higher level of authentication assurance. Section 15 FOIPPA - Disclosure harmful to law enforcement

Police Act – The *BC Police Act*, RSBC 1996, c.367 and the regulations thereto, all as amended from time to time.

Protected Information – Applies to information that if compromised could reasonably be expected to cause injury to a non-national interest – that is, an individual interest such as a person or an organization.[1]

> Protected "A": Applies to information that, if compromised, could cause injury to an individual, organization or government.
> Protected "B": Applies to information that, if compromised, could cause serious injury to an individual, organization or government *(i.e., PRIME records or medical records)*.
> Protected "C": Applies to information that, if compromised, could cause extremely grave injury to an individual, organization or government *(i.e., human source information)*.

Sensitive Information – Applies to information or assets that are more highly protected and, if compromised, could cause injury to an individual, the organization, government or other partners. For the purpose of this policy, 'sensitive information' is meant to include, but is not limited to TransLink confidential information. (*Note: Sensitive 'personal' information is not defined in the BC Freedom of Information and Protection of Privacy Act. Some types of personal information can be considered sensitive because there is a higher risk of harm to individuals if the information is improperly collected, used or disclosed (e.g., financial and health information)*.

[1] https://www.tpsgc-pwgsc.gc.ca/esc-src/protection-safeguarding/niveaux-levels-eng.html#s2; and https://www2.gov.bc.ca/assets/gov/government/services-for-government-and-broader-public-sector/information-technology-services/standards-files/information_security_classification_standard_july_17_2018.pdf

Transit Police IT Systems – For the purpose of this policy, the computing systems, related software and network facilities provided to Transit Police Personnel (and authorized Users) through the Transit Police.[2]

Transit Police Personnel – The sworn officers and civilian professionals of the Transit Police.

TransLink – The South Coast British Columbia Transportation Authority.

TSML – TransLink Security Management Limited, a subsidiary of the South Coast British Columbia Transportation Authority ("TransLink") and legal entity/employer for the Transit Police.

Wireless Access Points – A device that allows wireless devices to connect to a wired network using a Wi-Fi signal (e.g., wireless router).

Authority

1. Pursuant to the *Police Act*, the Chief Officer is responsible for the general supervision and command over the Transit Police, including implementing measures to ensure protection of the security and confidentiality interests of the Transit Police, its personnel, and law enforcement partners.

2. The Transit Police is permitted access to a number of regional, national and international law enforcement related information and technology records and systems, and must adhere to access security, confidentiality and information disclosure agreements and protocols.

3. TransLink has established a corporate policy ("Acceptable Use of Corporate Computing Systems") outlining the acceptable use of all TransLink provided computing hardware and software, and the corporate network facilities (collectively, the "Systems").TransLink recognizes that the Transit Police operates and maintains several systems specifically to fulfill the security and confidentiality requirements for a law enforcement organization, and must operate in compliance with the *Police Act*, *FOIPPA*, Transit Police and TSML policies, and other legal requirements. The provisions of the TransLink corporate policy are applicable to Transit Police (when using TransLink Systems) only to the extent that they do not conflict with any duties and obligations imposed on Transit Police by legislation, regulation, Transit Police or TSML policy, or other legal requirements. (If there is a conflict between requirements, the rules that are more stringent will be applied by Transit Police.)

4. The Transit Police is subject to the provisions of *FOIPPA* and under s. 30 of *FOIPPA* must protect personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.

[2] There are other IT systems managed and controlled by TransLink that are provided to Transit Police Personnel and TransLink's policy applies for access to those systems.

General

5. The Transit Police provides or facilitates access to computing systems to support the administrative and operational activities required to fulfill the organization's mandate. Strong access controls are important to the integrity and confidentiality of the Transit Police IT Systems. Depending on the level of access assigned to a system or User, weak access controls may result in inappropriate data disclosure, up to and including compromise of the Transit Police IT Systems and potentially that of a law enforcement partner regionally, nationally or internationally.

6. All Transit Police Personnel, its contractors, consultants and any other person with access to the Transit Police IT Systems ("Users") must exercise due diligence and adhere to the processes and protocols mandated by this and other policies in protecting the security of personal, law enforcement, and other sensitive information in the custody and control of the Transit Police. This policy will apply to all Users.

7. The Chief Officer will be responsible for ensuring organizational compliance with external requirements regarding the Transit Police protection of personal, law enforcement and other sensitive information within its care, custody and control, and will determine the internal accountability and measures necessary to achieve required compliance.

Accountability

8. Unless otherwise so determined by the Chief Officer, the Deputy Chief Officer Administrative Services will be responsible for ensuring that the Transit Police has in place the appropriate administrative, physical and technical safeguards for security of information within the care, custody and control of the Transit Police.

    (1) The measure of adequacy of these safeguards varies depending on the sensitivity of the information, the medium and format of the records, costs of security measures, the relationship between the Transit Police and affected individuals and/or agencies, including, but not limited to, interest in the data for criminal activity.

    NOTE: A failure to meet security/management requirements may lead to significant fines or loss of access to critical information management systems.

9. The Senior Manager Risk, Analytics and Emergency Planning, in coordination with the Privacy Officer, will be responsible for ensuring that there are periodic reviews of the privacy and security policies (including this policy chapter) in relation to personal and sensitive information under the custody and control of the Transit Police.

    NOTE: This review is in addition to those information reviews and audits that the Transit Police is already subject to under the Police Records Information Management Environment ("PRIME") and the Canadian Police Information Centre (CPIC).

10. With oversight by the Deputy Chief Officer Administrative Services, the Transit Police Information Technology Section ("IT Section") will be responsible for the administration of the Transit Police - IT Access Control Policy in relation to Transit Computing Systems in line with security requirements identified and accepted.

11. With oversight by the Deputy Chief Officer Administrative Services, and in consultation with the Privacy Officer, the Manager Information Management Services ("Manager IMS") will be responsible to:

    (1) Set the standards to manage and secure the personal information within the care, custody and control of the Transit Police;

    (2) Assess compliance with personal information privacy requirements; and

    (3) Conduct risk assessments of Transit Police personal information data banks at least annually and report to the Deputy Chief Officer Administrative Services on the result of these assessments.

Authorization

12. Only those persons authorized by the Chief Officer (or designate) will be permitted access to Transit Police IT Systems for access set-up, monitoring or audit purposes, or to ensure compliance with TransLink enterprise and TSML corporate policy.

13. Users requiring access to the Transit Police IT Systems will be issued account individual login credentials and a multi-factor authentication access, and must have a corresponding password that meets the approved password strength requirements, as set forth in this policy.

14. Transit Police Personnel will be provided training regarding administrative, physical and technical safeguards in place for security of information (including dissemination of information through encryption), as appropriate to their function with the Transit Police.

Violations

15. Any suspected access control policy violations or unauthorized activities involving the Transit Police IT Systems or Mobile Computing Devices will be reported to the IT Manager and Privacy Officer, who will then inform the Deputy Chief Officer Administrative Services and Supervisor (and Transit Police Professional Standards Unit as appropriate). Investigations of alleged misuse by Users will be conducted pursuant to requirements of the *Police Act*, *FOIPPA*, Transit Police and TSML policy, as applicable.

    (1) Any User found to have knowingly violated any portion of this policy may be subject to disciplinary action, up to and including termination of employment, cancellation of contract, and/or other legal remedies.

16. The IT Manager will take prompt action, from an IT system perspective, to address breaches of access control, consulting with the Privacy Officer.

17. The Deputy Chief Officer Administrative Services will immediately notify the Privacy Officer of any suspected or confirmed privacy breaches under s. 30 of the *FOIPPA* (if this has not already occurred from s. 15 above).

18. The Privacy Officer will ensure that privacy breach containment is implemented and that the Transit Police reports the breach pursuant to requirements of the *FOIPPA*. The Privacy Officer and Chief Officer or designate will notify other relevant persons/authorities and take actions in accordance with **TSML Policy No. 20 – Privacy Breach and Complaint Response** and the law.

19. The Deputy Chief Officer Administrative Services will direct a review of all violations to determine cause and any corrective action that can/should be taken. Violations will be reviewed as they are identified and appropriate action initiated, and in January of each year, a report will be prepared (covering the previous year) for the Chief Officer. The report will include an aggregate of all violations, actions taken in each case, trends identified and any recommendations for change to these policies and procedures.

Mobile Computing Devices

20. Due to the risks involved with sensitive information stored on Mobile Computing Devices, including loss and theft of such devices, security protection will be implemented by the Transit Police.

21. Transit Police Personnel will not normally store personal, law enforcement or other sensitive information on any Mobile Computing Device, except for temporary storage of such information on Transit Police authorized Mobile Computing Devices and in accordance with the access-control and security safeguards required for the specific information Section 15 FOIPPA - Disclosure harmful to law enforcement

    (1) As part of the IT equipment issuance process, the IT Section will install the appropriate security provisions to protect the data on the Mobile Computing Devices.

[Refer also to Transit Police SOP61 – Mobile Communication Devices, SOP73 – Portable Drives, and SOP86 – Two Factor Authentication – Pilot Project.]

22. Users will limit the amount of data stored on a Mobile Computing Device to that necessary for current operational purpose or retention requirements, taking into consideration s. 30 of *FOIPPA* regarding personal information, and frequently review what is being stored and delete unnecessary information. Secure disposal measures will be followed by Users.

23. When Transit Police Personnel are on leave of absence or extended leave (e.g., long term disability) of more than thirty days, Transit Police Personnel will be required to turn in all issued Mobile Computing Devices to their Supervisor.

Section 15 FOIPPA - Disclosure harmful to law enforcement

[redacted]
Section 15 FOIPPA - Disclosure harmful to law enforcement

24. The Supervisor will be responsible for ensuring that there are proper procedures in place for the safekeeping, security and continuity of the Mobile Computing Devices turned in by Transit Police Personnel pursuant to s. 23 of this policy.

[See also Transit Police policy chapter AC100 – Relinquishment of Issue Equipment]

Amendment

25. The Chief Officer will be authorized to issue policy and procedure amendments to the administrative, physical and technical safeguards (including access privileges and rights, and password and authentication requirements) necessary to maintain the security and confidentiality of the Transit Police IT Systems, to protect Transit Police Personnel, and to ensure compliance with law enforcement agreements and legislation.

PROCEDURES

Access Privileges and Rights

[redacted]
Section 15 FOIPPA - Disclosure harmful to law enforcement

[redacted]
Section 15 FOIPPA - Disclosure harmful to law enforcement
[redacted]

Access Passwords and Authentication

35. The Transit Police requires Users to comply with the following requirements regarding passwords and authentication for Transit Police IT Systems:

[redacted]
Section 15 FOIPPA - Disclosure harmful to law enforcement
[redacted]

Section 15 FOIPPA - Disclosure harmful to law enforcement

36. The IT Section (and project teams where appropriate) and Business Owners will be responsible for protecting their system-level passwords within a secured encrypted password management application or database.

Passwords for User Accounts

37. Users are required to comply with the following minimum requirements when setting 'User level' passwords for User Accounts. The password:

Section 15 FOIPPA - Disclosure harmful to law enforcement

38. Users account access will be locked after Section 15 FOIPPA - Disclosure harmful to law enforcement and the IT Section and Business Owners may implement technological measures to require Users to change their password or create a new account in order to achieve the next successful log on.

Passwords for System Accounts

39. The IT Section and Business Owners and/or system administrators will be required to comply with the following minimum requirements when setting 'System level' passwords for System Accounts. The password:

Section 15 FOIPPA - Disclosure harmful to law enforcement

40. The IT Section will ensure that new software and application deployments must have their default vendor passwords changed prior to use in the production environment at the Transit Police.

Passphrase for Transit Police Wireless Access Points

41. Users will follow the guidelines established by the IT Section for access to wireless access points. The IT Section setting of passphrases for wireless access points will:

Section 15 FOIPPA - Disclosure harmful to law enforcement

Computer Lockout

42. Unless otherwise so determined by the Deputy Chief Officer Administrative Services, all Transit Police computers will be configured to have a password-enabled screen saver lockout. This security feature will automatically initiate after the computer has remained idle from User interaction for five (5) minutes.

43. In addition to the five (5) minute automatic lockout feature, Transit Police recommends that Users log out (alternately, shut down or lock computers if a personal issue computer) when they leave the computer unattended. This prevents a period of vulnerability between time the User leaves and the time the locking screen saver is activated.

    NOTE: Users to use Ctrl/Alt/Delete and then "Enter" or click on Windows key and "L" to lock the computer (or use another lockout control available).

44. Following the screen saver lockout, the User will be required to re-enter their password and two-factor authentication to gain access to the computer.

Damaged, Stolen or Lost Tokens / 2FA Access

Section 15 FOIPPA - Disclosure harmful to law enforcement

[Refer to Transit Police policy chapter AG010 – Property Management]

Section 15 FOIPPA - Disclosure harmful to law enforcement

Off-Boarding

48. When off-boarding Transit Police Personnel, a record will be maintained by the IT Section of the completion of removal of access from the IT systems.

Audits

49. Audits of the IT access control will be as determined by the Transit Police Senior Manager Risk, Analytics and Emergency Planning, in consultation with the Manager IT.

REFERENCES

BC Freedom of Information and Protection of Privacy Act, RSBC 1996, c.165
BC Police Act, RSBC 1996, c.367
TransLink Policy: Acceptable Use of Corporate Computing Systems
TransLink Policy E-02: Information Security Governance NIST, Guide to Enterprise Password Management
Transit Police Policy Chapter AC100 – Relinquishment of Issue Equipment
Transit Police SOP86 – Two Factor Authentication – Pilot Project
Transit Police SOP61 – Mobile Communication Devices
Transit Police SOP73 – Portable Drives
TSML Policy No. 20 – Privacy Breach and Complaint Response