

Metro Trains Melbourne Pty Ltd (“Access Provider”)

Information Handling Protocol

1 Background

- 1.1 This protocol has been developed by the Access Provider in relation to access to the Network in accordance with the requirements of section 38ZZZB the *Rail Corporations Act* 1996 (Vic) (“Act”) and Guidelines made under the Act as at 1 January 2006.
- 1.2 The Access Provider reserves the right to amend this protocol in the event that the Act or the Guidelines are amended after 1 January 2006.
- 1.3 Any Operator who seeks access to the Network will be bound by this protocol.

2 Introduction

- 2.1 The Access Provider is required to establish and maintain a system and business rules relating to use or handling of confidential information provided by an Operator to the Access Provider and disclosure of that information by the Access Provider.
- 2.2 This protocol describes that system and those business rules.

3 Confidentiality

- 3.1 Confidential Information

The terms and conditions of all information provided by the Operator to the Access Provider under or in connection with the Train Path Request Process and Protocol (including the Access Arrangement Information) (the *Confidential Information*) are confidential.
- 3.2 Use of Confidential Information

The Access Provider must only use the Confidential Information for purposes connected with the Train Path Request Process and Protocol or purposes incidental to the Operator seeking access to the Network.
- 3.3 Prohibition of disclosure of Confidential Information

The Access Provider will ensure that it, its officers, employees, agents and subcontractors will not, without the consent (which consent will not unreasonably be withheld or delayed) of the

other party, disclose Confidential Information to any person, unless the disclosure:

- (a) is of Confidential Information already within the public domain other than as a result of a breach of this Process and Protocol or the Train Path Request Process and Protocol;
- (b) is of Confidential Information already known to that person (as evidenced by the person's written records) at the date of disclosure;
- (c) is to be made to the professional advisers (including legal and financial) of the Access Provider, provided that the disclosee agrees to keep the Confidential Information confidential;
- (d) subject to paragraph 3.4, is to be made to a Related Body Corporate of the Access Provider, provided that the disclosee agrees to keep the Confidential Information confidential;
- (e) is required by Law (including the Act or the Guidelines), or any Governmental Agency acting or purporting to act within its powers and functions, or by the requirements of Accreditation;
- (f) is reasonably necessary for the purposes of any mediation, expert determination, arbitration or legal proceeding involving the Access Provider or the Operator provided that (subject to any direction by the mediator, expert, arbitrator, appeal panel or court) the confidentiality of the information is maintained;
- (g) relates to information consisting of aggregate freight or aggregate passenger volume data for all operators or other aggregate usage statistics provided by the Operator to the Access Provider (but this does not permit the disclosure by the Access Provider of information relating to costs, payments, receipts or profits of the Operator);
- (h) is to the ACCC for the purposes of Part IIIA of the *Trade Practices Act 1974* (Cth) or to the ESC for the purposes of the Act or the Guidelines; or
- (i) is by the Access Provider to the manager of the Victorian country rail network for the purposes of managing the interface between the Network and the Victorian country rail network, provided that the disclosee agrees to keep the Confidential Information confidential.

3.4 Disclosure for purposes of this Process and Protocol

The Access Provider and the Operator must take all steps reasonably necessary to ensure that Confidential Information is disclosed only to such of its or its Related Body Corporate's officers, employees, agents or subcontractors who require that knowledge in order to carry out their duties in relation to the Train Path Request Process and Protocol.

3.5 Disclosure to State

Nothing in this paragraph 3 prevents the disclosure of Confidential Information to the Director or any minister, officer, employee, agent, adviser or consultant of the State of Victoria or a Governmental Agency of that State which has an enforceable right to such disclosure.

3.6 Confidentiality continues

The obligation of confidentiality under this paragraph is a continuing obligation and remains in force from the date upon which the Operator makes a request under paragraph 2.2 of the Train Path Request Process and Protocol.

4 Business Rules

These business rules are intended to enable the Access Provider to comply with its obligations of confidentiality under paragraph 3 and the Act.

4.1 Nominated Contact Officer

The Access Provider will nominate a person ("**Nominated Contact Officer**") who will be the point of contact with the Operator in connection with an Access Application.

4.2 Provision of Confidential Information by Operator

The Operator must only provide Confidential Information to the Access Provider:

- (a) in hard copy or in a sealed envelope or box marked to the attention of the Nominated Contact Officer; or
- (b) in electronic format sent only to the Nominated Contact Officer; and
- (c) clearly marked as "Commercial in Confidence".

4.3 Responsibilities of Nominated Contact Officer

The Nominated Contact Officer is responsible for:

- (a) maintenance of a register identifying any Confidential Information received from the Operator, any copies made, which of the Access Provider's officers, employees, agents, subcontractors, professional advisers (including legal and financial) or Related Bodies

Corporate have received the Confidential Information and from whom it has been retrieved, storage location, archive location and destruction date.

- (b) distribution of Confidential information to persons or entities entitled to that information in accordance with paragraph 3;
- (c) control of copying of the Confidential Information by the Access Provider;
- (d) storing Confidential Information that is in electronic format in a secure manner on the Access Provider's Computer system including control of passwords;
- (e) recovery, filing and destruction of Confidential Information held by the Access Provider, and
- (f) maintaining the register described in paragraph 4.9, in accordance with these business rules.

4.4 Security of Confidential Information

The Access Provider must store Confidential Information in a secure manner, including:

- (a) hard copy information must be kept in a locked cabinet when it is not being used;
- (b) information in electronic format must be stored in a "password protected" file in the Access Provider's computer system and the protocols in paragraph 4.11 will apply;
- (c) access for the Access Provider's staff is limited only to persons specifically authorised by the Nominated Contact Officer;
- (d) no copying is permitted except by the Nominated Contact Officer or under his or her control;
- (e) disclosure as contemplated by paragraphs 3.3(c), (d) or (i) will not be made unless the relevant disclosee has first executed a confidentiality undertaking in favour of the Access Provider;
- (f) the information will only be available to persons or entities to whom the Access Provider is entitled to provide the information in accordance with paragraph 3; and
- (g) disclosure under paragraphs 3.3(e) or (h) will only be made upon the written request of the relevant disclosee.

4.5 Informing Operator of Disclosure

If the Access Provider makes a disclosure of Confidential Information as permitted by paragraphs 3.3(e) or (h) or paragraph 3.4 it will notify the Operator within 24 hours of the disclosure.

4.6 Return or Destruction of Confidential Information

Subject to paragraph 4.7, if the Operator so requests in writing, the Access Provider will at the cost of the Operator, return or (at the option of the Access Provider) destroy all copies of the Confidential Information within its possession.

4.7 Access Provider Entitlement to Retain Copies

Notwithstanding paragraph 4.6, the Access Provider is entitled to retain a copy or copies of any Confidential Information:

- (a) that is contained or included in the board records of the Access Provider;
- (b) to the extent required by any Law;
- (c) to the extent necessary to enable it to comply with any obligation owed by the Access Provider to the Director or a Governmental Agency;
- (d) for the purposes of any mediation, expert determination, arbitration or legal proceeding involving the Access Provider or its officers, employees, agents or subcontractors; or
- (e) as required by the auditors of the Access Provider.

4.8 Destruction Option

The Access Provider may elect to destroy all or any part of the Confidential Information at any time and is not obliged to retain any such information.

4.9 Records of Disclosure

The Nominated Contact Officer will retain a register of any disclosures of the Confidential Information made under clauses 3.2(e), 3(f), 3(h) or 3.4. The Operator may obtain a copy of that register upon written request.

4.10 Incident Reporting/Corrective Action

The Nominated Contact Officer must immediately report to the Company Secretary of the Access Provider if he or she discovers or suspects that a breach of these business rules may have occurred. The Company Secretary must refer the matter to the Chief Executive Officer and initiate corrective action, which may include disciplinary proceedings against the person who may have breached these business rules. If the Access Provider becomes aware of a breach by the Nominated Contact Officer of this protocol, the Access Provider must take corrective action which may include:

- (a) disciplinary proceedings against the Nominated Contract Officer; and/or
- (b) removal of the person occupying the position of Nominated Contact Officer from his or her position and replacement with a new Nominated Contact Officer.

4.11 IT Security

In order to preserve the security of any Confidential information held by the Access Provider in electronic format, the following protocols will be observed in connection with the Access Provider's IT system:

- (a) Confidential Information will be stored in a file on a network drive that is only accessible by a user logging in using a secure password;
- (b) a secure password may only be allocated to a user by the Nominated Contact Person;
- (c) if a user is no longer entitled to access the Confidential Information, the IT system must be updated to cancel access from that password;
- (d) the Access Provider's IT system will record and the Nominated Contact Person will be informed of any attempted or actual log-in activity on the relevant site.

5 Glossary

In this document the following definitions apply unless the context requires otherwise.

"access" means access to the Network or part of the Network, to operate freight services or passenger services.

"Access Application" means an application for access by an Operator under the Train Path Request Process and Protocol.

"Access Arrangement Information" means information that the Access Provider is required to provide to the Operator under the Guidelines and the Act.

"Access Provider" means Metro Trains Melbourne Pty Ltd ACN 136 429 948.

"Accreditation" means accreditation obtained in accordance with the requirements of Division 3, Part VI of the Transport Act, including any guideline, regulation or ordinance made pursuant to that Division.

"Act" means the *Rail Corporations Act 2002 (Vic)*.

"Business Day" means a week day on which trading banks are open in Melbourne.

“**Director**” means the Director of Public Transport under the *Transport Act 1983* (Vic).

“**ESC**” means the Essential Services Commission or its successor.

“**Governmental Agency**” means any government or any governmental, semi-governmental or judicial entity or authority, including any self regulatory organisation or any stock exchange.

“**Guidelines**” means the guidelines made by the ESC under the Act.

“**Infrastructure Lease**” means the lease titled “Infrastructure Lease - Train” between the Director, VRTC and the Access Provider dated 31 August 2009, as amended.

“**Law**” means any statute, regulation, order, rule, subordinate legislation or other document enforceable under any statute, regulation, order, rule or subordinate legislation.

“**Network**” means the land and infrastructure leased by the Access Provider under the Infrastructure Lease from time to time, including railway track, associated track structures and works (such as cuttings, tunnels, bridges, sidings, excavations, landfill, track support earthworks and drainage works), pedestrian crossings, over-track structures, under-track structures, service roads, signalling, notices and signs and overhead electrical power supply systems, but excluding:

- (a) buildings (including stations, platforms, sheds and shelters);
- (b) carparks;
- (c) terminals, storage and receival facilities;
- (d) workshops, depots, yards and fuel points; and
- (e) private sidings that are not leased to the Access Provider,

but includes any infrastructure leased to the Access Provider which passes through, or is immediately adjacent to, any of the infrastructure or facilities referred to in paragraphs (a) to (e) above.

“**Nominated Contact Officer**” has the meaning given in paragraph 4.2.

“**Operator**” means the person seeking access to or having a legally enforceable right to have access to the Network.

“**Related Body Corporate**” has the meaning given in the *Corporations Act 2001* (Cth).

“**Train Path**” means the particular time interval, including an entry time and day and an exit time and day, through which rolling stock may travel over a section of the Network from an origin to a destination (including stopping points).

“**VRTC**” means Victorian Rail Track Corporation.