



Road Traffic
Management Corporation

**MANUAL ON THE PROMOTION
OF
ACCESS TO INFORMATION ACT, 2000**

THE PURPOSE AND INTENT OF THIS MANUAL

The purpose of this manual is primarily to provide a background to the Road Traffic Management Corporation as a public body and furthermore provide the procedure to access records held and in the custody of the Road Traffic Management Corporation, It also aims to provide a description of personal information held by the Road Traffic Management Corporation and outlines the rights of the data subject. This manual can be accessed on the Road Traffic Management Corporation and Natis website or can be requested from the Deputy Information Officer by email or from Road Traffic Management Corporation's Head Office. Should you have any difficulty in making use this manual, please contact the Deputy Information Officer who will assist you further. The Road Traffic Management Corporation fully subscribes to the spirit and letter of the Promotion of Access to Information Act ("PAIA") as well as the Protection of Information Act 4 of 2013 ("POPIA") and wishes to foster a culture of transparency and accountability.

THE RTMC – BACKGROUND INFORMATION

1.1 INTRODUCTION

The RTMC was established in terms of section 3 of the Road Traffic Management Corporation Act, Act 20 of 1999 (“RTMC Act”) and listed as a Schedule 3A public entity in terms of the Public Finance Management Act No 1 of 1999.

The RTMC Act was approved by Parliament in 1999 with the main purpose of pooling powers and resources to eliminate the fragmentation of responsibilities for all aspects of road traffic management across the various levels of Government.

The mandate of the RTMC is derived from the provisions of the RTMC Act, which provides, in the public interest, for co-operative and coordinated strategic planning, regulation, facilitation and law enforcement in respect of road traffic matters by the national, provincial and local spheres of Government.

1.2 VISION, MISSION AND VALUES OF THE RTMC

1.2.1 Vision – Safe Roads in South Africa

1.2.2 Mission - Ensure safe, secure and responsible use of roads in South Africa through:

- a. Education
- b. Enforcement
- c. Engineering
- d. Evaluation
- e. Planning and Coordination
- f. Partnerships

1.2.3 Values - The core values of the RTMC are:

- a. Integrity
- b. Accountability
- c. Transparency
- d. Teamwork

1.3 KEY OBJECTIVES OF THE RTMC

- 1.3.1 To establish the RTMC as a partner between national, provincial and local spheres of government;
- 1.3.2 To enhance the overall quality of road traffic service provision to ensure safety, security, order, discipline and mobility on the roads;
- 1.3.3 To protect road infrastructure and the environment through the adoption of innovative practices and implementation of innovative technology;
- 1.3.4 To phase out, where appropriate, public funding and phase in private sector investment in road traffic on a competitive basis;
- 1.3.5 To introduce commercial management principles to inform and guide road traffic governance and decision-making in the interest of enhanced service provision;
- 1.3.6 To optimise the utilisation of public funds by:
 - a. Limiting investment of public funds to road traffic services which meet a social or non-commercial strategic objective, and which have poor potential to generate a reasonable rate of return; and
 - b. Securing, where appropriate, full cost recovery based on the user-pays principle.
- 1.3.7 To regulate, strengthen and monitor inter-governmental contact and cooperation in road traffic matters;
- 1.3.8 To improve the exchange and dissemination of information on road traffic matters;
- 1.3.9 To stimulate research in road traffic matters and effectively use the resources of existing institutes and research bodies; and
- 1.3.10 To develop human resources in the public and private sectors that are involved in road traffic.

1.4 GOVERNANCE STRUCTURES OF THE RTMC

The RTMC governance structure comprises of:

- 1.4.1 The Shareholders Committee;
- 1.4.2 The Board of Directors;
- 1.4.3 Audit and Risk Committee;
- 1.4.4 Strategy, Monitoring and Evaluation Committee;
- 1.4.5 Social and Ethics Committee
- 1.4.6 Remuneration Committee
- 1.4.7 Executive Committee

1.5 FUNCTIONAL UNITS OF THE RTMC

1.5.1 OFFICE OF THE CHIEF EXECUTIVE

a) CEO Office

To manage and oversee the functions, staff and resources of the Corporation in line with the RTMC Act and assume overall strategic, managerial, functional and operational responsibility for the Corporation.

b) Communications

The unit is responsible for developing and maintaining the Corporation's media strategy and plan. The incumbent will also be responsible for managing the reputation of the Corporation and deal with any media issues.

(c) National Traffic Anti-Corruption Unit

The main aim of the incumbents in the structure is to identify, analyse and investigate any corruption activities in the traffic transport sector and to eliminate fraud and corruption within national, provincial and local road traffic fraternity by ensuring the safety of all drivers, vehicles and road users who are using the country's roads.

(d) Internal Audit

The primary purpose of internal audit is to provide reasonable assurance that the system of internal control implemented by management is adequate and effective in order to manage risks and maintain effective financial control within limits acceptable to management. In the process, internal audit will also provide advisory services on how to improve on deficient controls.

(e) Company Secretary

The role and responsibilities of the Office of the Company secretariat is guided by the provisions of the Companies Act, 2016, section 88 in particular as well as the principles and practices recommended in King IV Code on Corporate Governance. This includes, amongst others, the following:

- i) Providing the directors collectively and individually with guidance as to their fiduciary duties, responsibilities and powers.
- ii) Making directors aware of laws and regulations relevant and/or affecting the company.
- iii) Monitoring the developments on best practice in respect of corporate governance and bring these to the Board's attention where they would add value.
- iv) Provide administrative support and performance of secretariat functions to the Shareholders Committee, as outlined in section 17 of the Road Traffic Management Cooperation Act, 1999 (Act No. 20 of 1999) as amended.

(f) Organisational Strategy

The main function of the department is to manage the planning and reporting processes regarding the RTMC's strategy. The function of Monitoring and Evaluation is also situated in this department.

(g) Programme Management Office

The main function of this Department is the development of a Programme and Project Management framework for the Corporation and then ensuring compliance with these set frameworks, policies and procedures.

(h) Organisational Risk

The main functions of the Department will be to develop the Enterprise-Wide Risk Management Framework and plan and ensure that this is implemented throughout the Corporation. The development of and ensuring compliance with the business continuity management and disaster recovery plan is also embedded in this function.

(i) Law Enforcement Norms and Standards

Law Enforcement Norms, Standard and Inspectorate coordinates and collaborates with other authorities in the development and monitoring of implementation of road traffic law enforcement norms and standards throughout the three spheres of government. The monitoring function will be achieved through the Road Traffic Law Enforcement Inspectorate unit which is responsible for physical inspections of traffic authorities, traffic activities, events, and projects.

1.1.1 TRAFFIC LAW ENFORCEMENT

The Unit provides road traffic law enforcement services through the National Road Traffic Police Unit and are responsible for the strategic, operational and monitoring of the law enforcement services rendered by the unit and traffic officers.

1.1.2 ROAD SAFETY, STAKEHOLDER RELATIONS MANAGEMENT, MARKETING & COMMUNICATION

The main objective of the Road Safety business unit is to contribute towards safer roads in the country through education and awareness programmes in all provincial and local spheres of government departments. These include stakeholders responsible for traffic and road safety including local authorities, transport entities as well private sector and NGOs.

(a) Road Safety Programmes

The Road Safety unit further provides strategic leadership in the road safety sector through overseeing the implementation of the Nation Road Safety Strategy 2016 - 2030. The Unit is also responsible for promoting safer road conduct by all categories of road users in the country. This is done through formal and informal means of knowledge transfer and practise using specific programmes and projects.

(b) Intergovernmental Relations

The Stakeholder Relations components are managed within Road Safety (in soliciting funding from the provide sector) for Road Safety, Law Enforcement and Traffic Training) whilst the Intergovernmental Relations (IGR) unit is key the establishment of new relationships between public sector stakeholders and the Corporation as well as being crucial in providing strategic support to business units in resolving issues with stakeholders.

(c) Marketing

The Marketing business unit is a support function, in which events, graphic design and multi-media services are provided to the Corporation. This includes and not limited to, the use of the entity's corporate image elements branding items, critical report design work and advertorial work at large. The Marketing business unit is also responsible for the implementation of Corporation Social Responsibility (CSR) programmes, in which the Corporation plays an important role in the socio-economic transformation of its stakeholders and communities in the South Africa, with the key objective of facilitating sustainable development and self-sufficiency programmes.

1.5.4 ROAD TRAFFIC TRAINING ACADEMY

(a) Administration and Learner Support

The Administration and Learner Support function of the Road Traffic Training Academy is responsible for ensuring that all administrative and learner support processes and systems are developed and that all learners at the Colleges are properly supported throughout the training process.

(b) Training Delivery

The Training Delivery sub-unit is responsible for ensuring that all training delivery at the Academy happens within set requirements and to further oversee the facilitation and delivery of traffic training at the Academy.

(c) Training Material Development and Quality Assurance and Quality Assurance

The Training Material Development and Quality Assurance and Quality Assurance sub-unit is responsible for ensuring that all training and assessment material is developed based on the qualification and curriculum requirements and ensuring that the training material, assessments and actual training processes are quality assured.

1.5.5 ROAD TRAFFIC INFORMATION & TECHNOLOGY

(a) Information Governance and Security

The main functions are:

- Ensure that all information systems, networks and information are secure;
- Ensure that there is compliance from all Natis end users; and
- Register and control access to Natis and other systems.

(b) Research and Innovation

The unit is responsible for ensuring that all relevant road traffic and road safety research is properly gathered, investigated, analysed, packaged and provided to relevant internal and external stakeholders. The incumbent is also responsible for ensuring that Road Traffic Safety Engineering processes is managed across the country and along regional corridors.

(c) Road Traffic Information

The main functions are:

- Ensure that all relevant road traffic and accident information and statistics are properly and securely gathered, captured, verified and analysed; and
- Ensure that relevant reports are compiled, packaged and distributed to internal and external stakeholders.

(d) Road Traffic Information Systems

The main functions are:

- Ensure that all demands from users are identified and that business intelligence regarding needs are available;
- Ensure that a proper analysis of all needs is done and that relevant technical specification documents are developed;
- Ensure the development of software / applications based on all identified specifications;
- Ensure that all newly developed software is quality assured; and
- Ensure that projects are managed properly.

(e) Road Traffic Management Infrastructure

The unit is responsible for the provision and management of the IT infrastructure operations ensuring an effective, efficient and best value IT service is provided.

(f) Road Traffic Management Systems Support

The main functions are:

- provide first line support to internal and external users through different ways, e.g., service desk, technical support or call center.
- supply technical support to provinces, municipal offices and SAPO offices where RTMC equipment (Natis) is used.
- ensure that Natis sites are properly identified and logged, that all IT assets and logistics are dealt with and that equipment is properly deployed.
- provide Natis Application training to Natis Users.

1.5.6 SUPPORT UNITS OF THE RTMC

CORPORATE SERVICES

(a) Training Norms and Standards Unit

This Unit focuses on the overall quality of road traffic training, determining and implementing standards for training of traffic and road safety personnel. This function involves receiving and verification of personal documents and qualifications for enrolled learners for the various courses to be verified to check compliance with the Policy Document for Traffic Training Centres. It also involves receiving and quality assurance of facilitators/ lecturers personal documents and qualification to check compliance.

(b) Human Capital

Human resource management ensures optimum and efficient use and development of human capital and provides an advisory service on organisational effectiveness and development, individual performance management as well as effective and efficient recruitment, selection and placement services such as benchmarking, and development of human resources policies and practices. In accordance with the approved structure, the human resources function comprises organisational development and human resource operations.

(c) Transformation and Employee Relations

There are three main functions in the department namely: Labour Relations, Transformation and Employee Wellness

(d) Legal and Compliance Services

This unit's key functions are to render professional, reliable, effective and efficient legal services to the Corporation and to monitor the Compliance of the Corporation.

(e) Total Facilities Management

The Total Facilities Management Department of different Units, namely, Knowledge Management, Security and OHS Management, Fleet Management and Facilities Management. The unit is responsible for

- ensuring that all information in the Corporation is kept safe and secure and is managed properly.
- ensuring that a proper records management system and archiving process is applied throughout the Corporation.
- Switchboard, Reception, Messenger and Driving functions.
- oversee work done in different buildings and deal with some of the services delivered in the different buildings.
- responsible for managing Cleaners, Grounds Men and Maintenance Technicians.
- any maintenance related work and contracts at the different buildings.
- OHS, Vetting and Screening, Integrated Electronic Security, Prevention, Detection and Analysis as well as Physical Security.
- ensuring that security risks in processes, systems and facilities are identified and analysed and corrective actions proposed.
- ensure that all related security functions are implemented.
- ensuring that the fleet of vehicles are managed and coordinated properly

(f) Operational Secretariat Services

The unit provides secretariat and administrative support services to the Corporation, mainly for institutional governance structures as well as ad-hoc meeting as per the directive of the Chief Executive Officer. The unit ensure the effective and efficient operation of RTMC governance structures and provide support for participation in external structures.

1.5.7 FINANCIAL SERVICES

Unit renders an effective and professional Financial Management Service to the Corporation which includes:

- Improving financial performance, practice, and fiscal discipline
- Managing and executing financial management
- Ensuring clean and unqualified annual financial statements
- Executing risk management and internal control systems
- Managing and executing supply chain management
- Executing revenue management
- Managing and executing asset management
- Providing Budget management

PROMOTION OF ACCESS TO INFORMATION ACT (PAIA) AND PROTECTION OF PERSONAL INFORMATION (POPI) ACT

2.1 PAIA

- 2.1.1 PAIA was enacted in 2000 to give effect to section 32 of the Constitution of the Republic of South Africa, 108 of 1990, which provides that everyone has the right of access to any information held by the State and any information that is held by another person and that is required for the exercise or protection of any rights.
- 2.1.2 PAIA came into effect on 9 March 2001 with the exception of sections 10, 14, 16 and 51 which sections were brought into operation on 15 February 2002.
- 2.1.3 PAIA affords natural and/or juristic persons the right of access to records held by either a private or public body, subject to certain limitations, in order to enable them to exercise or protect their rights.
- 2.1.4 Where a request is made in terms of PAIA, the RTMC is obliged to release the information, except where PAIA expressly provides that the information must not be released. The Act sets out the requisite procedural issues attached to such request.

2.2 POPIA

- 2.2.1 Previously, South Africa did not have legislation dealing specifically and exclusively with data protection. Hence, to give effect to the Constitutional right to privacy, on 20 August 2013, the National Assembly passed the Protection of Personal Information Bill [B9D of 2009].
- 2.2.2 The Bill was signed into law by the President on 19 November 2013 and was gazetted as the Protection of Personal Information Act 4 of 2013 (POPIA) on 26 November 2013.
- 2.2.3 Sections 2 to 38; sections 55 to 109; section 111; and section 114(1), (2) and (3) of POPIA came into force on 1 July 2020.
- 2.2.4 Sections 110 and 114(4) shall commence on 30 June 2021.

- 2.2.5 Certain provisions relating to the establishment of the Information Regulator and the making of Regulations under POPIA have, however, come into force on 11 April 2014. The Regulator was appointed on 1 December 2016 and the draft Regulations were published on 8 September 2017.
- 2.2.6 POPIA affords data subjects the right to request access to their personal information from any responsible party.
- 2.2.7 Any information processing by the RTMC, including the release of NaTIS information, must comply with the provisions of POPIA.
- 2.2.8 POPIA requires the RTMC to inform data subjects as to the manner in which their personal information is used, disclosed and the like.
- 2.2.9 The RTMC guarantees its commitment to protecting the privacy of data subjects and ensuring that their personal information is used appropriately, transparently, securely and in accordance with applicable laws.

3. RECORDS OF INFORMATION HELD BY THE RTMC

The following are subjects and categories of records held by the RTMC:

3.1 RECORDS AUTOMATICALLY AVAILABLE

In terms of section 14(1)(e) of the Act, the Department has the following categories of the records that are automatically available for copying and inspection without a person having to request access in terms of PAIA:

- (a) Acts, Bills and Regulations published by the Department;
- (b) published policies and guidelines;
- (c) application forms;
- (d) contact directory;
- (e) e-publications;
- (f) published booklets and brochures;
- (g) published marketing material, including departmental marketing brochures;
- (h) published newsletters;
- (i) published posters and pamphlets;
- (j) published reports;
- (k) strategic plan;
- (l) annual performance plans;
- (m) annual reports;
- (n) budget speeches;
- (o) vacancy circulars;
- (p) collective bargaining agreements;

(q) Finance -

- Procurement Plans
- Bid documents
- Tender adverts,
- SCM Legislation
- Received bids
- Awarded bids
- Budget Information
- Financial Statements and

(r) Training Norms and Standards Unit

- Enrolment details of trainees for Authorised Officers' courses as Traffic Training Centres
- Assessment request for Authorised Officer's Courses from Traffic Training Centres
- Moderation and Traffic College Evaluation Reports

(s) Notwithstanding the exceptions in granting access to NaTIS Information, RTMC discloses statistical information voluntarily for the sake of transparency and convenience to the public.

The following categories of information are available on our website www.enatis.com free of charge and without submitting a formal request.

Category of information	Description
a. Live Vehicle Population	Detailed statistics on South Africa's live vehicle population as reflected on the NaTIS, including month-to-month increases and decreases
b. New Vehicle Registrations	Detailed statistics on new vehicle registrations recorded on the NaTIS, including year-on-year comparisons
c. Used Vehicle Registrations	Detailed statistics of used vehicle registrations as recorded on the NaTIS, including year-on-year comparisons
d. Live Vehicle Population per Registering Authority	Detailed statistics on South Africa's live vehicle population per Registering Authority as reflected on the NaTIS, including month-to-month increases and decreases
e. Driver Licence Population	Detailed statistics on South African driver licence population as reflected on the NaTIS

3.2 RECORDS TO BE FORMALLY REQUESTED

3.2.1 OFFICE OF THE CEO

(a) CEO Office

The unit keep this information manually and aiming at introducing a digital system in future. The documents listed below are available on request from the RTMC.

- Investigation Reports.
- POE on investigation files.

(b) Communications

Internal submissions, memorandums and communication.

(c) National Traffic Anti-Corruption Unit

- Investigation (ongoing and completed) Reports;
- Criminal Litigation Reports and files
- Internal submissions, memorandums and communication.

(d) Internal Audit

The primary purpose of internal audit is to provide reasonable assurance that the system of internal control implemented by management is adequate and effective in order to manage risks and maintain effective financial control within limits acceptable to management. In the process, internal audit will also provide advisory services on how to improve on deficient controls.

(e) Company Secretary

Board and Board Sub Committee Minutes

(f) Organisational Strategy

- Internal submissions, memorandums and communication.
- Internal Reports

(g) Programme Management Office

- Internal submissions, memorandums, and communication
- Programme Management Status Reports (monthly, quarterly and annually)

(h) Organisational Risk

- Internal submissions, memorandums and communication.
- Internal Risk reports and registers

(i) Law Enforcement Norms and Standards

- Internal Submissions, memorandums and
- Unpublished Audit Reports

3.2.2 LAW ENFORCEMENT

Records to be formally requested

The unit keeps this information, mainly manual, and is looking at introducing an electronic system in future. The documents listed below are available on request from the RTMC.

- Road Traffic Law Enforcement Policy Documents: Includes documents developed with the Expert Standard development working group comprising of representatives from provinces and chaired by the RTMC.
- Road Traffic Law Enforcement Standards: Standards that are developed to guide operations within traffic law enforcement in the country.
- National Road Traffic Law Enforcement Code: A document developed with the intention of bring harmonisation and standardization within traffic law enforcement in the country, This document is available in print form as well as electronically and is applicable to all officers and authorities.
- Reports (Inspectorate) etc: There are inspection reports that are compiled after physical inspections of law enforcement operations have been conducted.
- Traffic Law Enforcement Equipment Register: The unit compiles the equipment register and ensures that law enforcement equipment is registered with the relevant professional body.
- Traffic Law Enforcement Officers Register: The Unit maintains traffic officers register to ensure that officers are correctly registered within the relevant legislations and policies.
- Traffic Law Enforcement equipment service providers: The unit compiles the service providers register and ensures that they comply with the relevant legislations and policies.
- Traffic Law Enforcement Fixed Speed Monitoring Locations: The unit compiles the fixed speed monitoring device's locations and ensures that they comply with the relevant legislations and policies.
- Traffic Law Enforcement Authorities Register: The unit compiles the law enforcement authorities register and ensures that they comply with the relevant legislations and policies.
- Traffic Law Enforcement two-radio Register: The unit compiles the national authority two-way radio register and ensures that they comply with the relevant legislations and policies.

3.2.3 ROAD SAFETY, STAKEHOLDER RELATIONS MANAGEMENT, MARKETING & COMMUNICATION

- Internal submissions, memorandums and communication.
- Internal Reports

3.2.4 ROAD TRAFFIC TRAINING ACADEMY

(a) Administration and Learner Support

- Training programme for a calendar year for the Examiner of Vehicles, Examiner Drivers Licenses and Traffic Officers);
- Enquiries on Refresher Courses for these EOVS, EDL, Peace Officer and Traffic Officers);
- The cost for training courses;
- Duration of the courses;
- The intake of the Traffic Officers Learnership and how long the training takes;
- The College SASSETA registration number;
- SASSETA Unit Standard registered numbers;
- Confirmation of the results (statement of results);
- Request for duplicate qualifications;
- The request for quotations and invoices of courses;
- Information pertaining to whether an individual can do the course or through an Employer;
- Request for utilisation of facilities such as the skid-pan, shooting range and K53 yard test.
- Enrolment details of trainees for Authorised Officers' courses as Traffic Training Centres;
- Academy prospectus;
- Induction and Orientation Process Manual;
- Learner Information Management System Records;
- Portfolios of Evidence of enrolled and previous trainees;
- Verification of authenticity of qualifications;
- Sub-unit specific Policies, Frameworks and Standard Operating Procedures (i.e., Administration, Library Services and Learner Support);
- Business Cases for sourcing of goods and services related to training;

(b) Training Delivery

- Training time-table;
- Assessment Schedule;
- Post-training Evaluation Forms;
- Training Agreement;
- Learner Code of Conduct;
- Standard Operating Procedures (College Rules);
- Disciplinary Code of Conduct;

(c) Training Material Development and Quality Assurance

- Quality Management System Document;
- Training material including learner guides, assessment guides, facilitator guides and learner workbooks;
- Internal quality assurance manual and procedures;
- Internal moderation manual and procedures;
- Internal moderation plans;
- Internal moderation checklists;
- Internal moderation reports;
- Internal quality assurance audits;
- Internal quality assurance reports; and
- Standard Operating Procedures (Training Material Development).

3.2.5 ROAD TRAFFIC INFORMATION & TECHNOLOGY

The National Traffic Information System (NaTIS) is the integrated functionary tool and is comprised of the National Traffic System, National Operator System and National Contravention System. Incorporated in these systems are Road Traffic Registers as defined in the National Road Traffic Regulations. Protecting access to the NaTIS is critical in maintaining the integrity of data stored and processed by our information systems and in preventing unauthorised access to such systems.

Access to the Corporation's information systems must be restricted to only authorised Third-Parties or processes, based on the Principles of Need to Know and Least Privilege:

- i) Prior to granting access to NaTIS information, a due diligence exercise aimed at establishing, among other things, requestor's identity, their business activities, source of funds and physical location must be conducted (Know Your Client).
- ii) Prior to granting access to NaTIS information, the different means, and controls to be implemented by the requestor when storing, processing, communicating, sharing, exchanging, and disposing of NaTIS information must be established. Information flow diagrams depicting the flow of NaTIS information must be developed.
- iii) Prior to granting access to NaTIS information, the value of this information and its criticality to the business operations of the requestor must be determined.
- iv) Prior to granting access to NaTIS information, all required documentation must be completed and signed at the correct level, including agreements.
- v) When granting access to NaTIS information, the Principle of Least Privilege (POLP) must apply to limit access rights to the bare minimum permissions the requestor needs to perform their business operations.
- vii) All agreements and related documents must include the Right of Audit clause to empower the Corporation to perform ongoing monitoring of compliance and evaluation of controls implemented by the requestor.
- viii) Periodic evaluation of internal controls implemented by the Corporation to protect NaTIS information that is not intended to be accessible to unauthorised individuals must be performed.
- ix) Periodic evaluation of controls implemented by the requestor to protect NaTIS information must be performed. It must be ensured that requestors implement recommended actions emanating from these evaluations.
- x) No specific vehicle information such as full vehicle identification number (VIN), and engine number must be provided to Third-party entities.
- xi) Access to NaTIS for the purpose of reselling the information is strictly prohibited.

- xii) Information obtained from NaTIS may not be disseminated to other entities, unless the condition of access issued by the Corporation expressly permits the dissemination of NaTIS information to other parties.

Given the broad definition of “personal information” in the Promotion of Access to Information Act (PAIA) as well as in the Protection of Personal Information (POPI) Act, balancing privacy with freedom of access to information becomes very important.

A determination must, however, be made to consider whether the personal information in question falls into the following categories of personal information, which may be disclosed:

- i) Personal information of an individual who has given consent for this information to be released.
- ii) Personal information which has already been made public.
- iii) Personal information about a child under the age of 18 where the disclosure of such information is in the best interest of the child, and the requestor is the child’s parent or guardian.
- iv) Personal information of a deceased person to a requestor who is the individual’s next of kin, or who has been authorised (written consent) by the next of kin.
- v) Personal information of a deceased person who has been deceased for a period of more than 20 years.
- vii) Personal information of an individual who is or was an official in a public or private body and where the information relates to their position as an official.

The classification of requestors for NaTis are classified into two broad categories as follows:

A: Designated Entities

These are the entities that contribute to the NaTIS Information by introducing records of new vehicles, imported vehicles and new trailers to the NaTIS by means of an interface (directly) or through a municipality (indirectly).

The Designated entities are described as follows:

i) Registering Authorities, Public Vehicle Testing Stations and Driving Licence Testing Centres

All registering authorities, vehicle testing stations under the control of the registering authority and driving licence testing centres appointed in terms of Section 3 and 8 respectively, will be granted direct access to the NaTIS to execute their function.

It is the duty of the province concerned to inform the Corporation of the appointment of such registering authority.

ii) State Departments and their Agents

All State Departments and their Agencies may apply to the Corporation for access by completing the Access to NaTIS Information (ANI) form. Such access shall be subject to the conclusion of a Memorandum of Understanding (MOU) between the Corporation and the Entity, which will set out the nature of the information required, the obligations of the parties and the protection of personal information as prescribed.

iii) Manufacturers, Importers and Builders of motor vehicles

The provincial department of transport shall notify the Corporation to grant access to a Manufacturer, Importer or Builder (MIB), registered in terms of Section 5 of the Act, for the purpose of introduction and releasing of new motor vehicles for sale in the Republic.

The Corporation shall require the MIB to complete the Access to NaTIS Information (ANI) form prior to granting access in terms of the Onboarding of Manufacturers, Importers and Builders (MIB) procedure.

iv) Motor Vehicle Financing and Insurance Companies

Motor Vehicle Financing and Insurance Companies may apply to the Corporation for access by completing the ANI form. Such access shall be subject to the conclusion of a Service Level Agreement (SLA) between the Corporation and the Entity, which will set out the nature of the information required, the obligations of the parties and the protection of personal information as prescribed.

Access provided in terms of this paragraph shall be limited to the prevention of fraud related to motor vehicle finance and insurance only.

v) Entities or Individuals conducting Research relating to Road Traffic Management

Academic Institutions may apply to the Corporation for access by completing the ANI form. Such access shall be subject to the conclusion of a Memorandum of Understanding (MOU) between the Corporation and the Entities that will set out the nature of the information required, the obligations of the parties and the protection of personal information as prescribed.

The Corporation's Research and Innovation Division will be required to endorse the application in so far as the research relates to the Road Traffic Management.

Access provided in terms of this paragraph shall be limited to the research topic.

vi) Private Vehicle Testing Stations

The Provincial Department of Transport shall notify the Corporation of the registration of a Private Vehicle Testing Station (PVTs) and request access after the registration of such PVTs in terms of section 38 of the Act.

The Corporation shall require the PVTs to complete the necessary documentation prior to granting access in terms of the Onboarding of Private Vehicle Testing Stations (PVTs) procedure.

Suitable network access connectivity shall be determined by the Corporation in terms of the Network Standard for Direct Access.

vii) Traffic Law Enforcement Authorities

Traffic Law Enforcement Authorities (TLEAs) must complete the ANI form for access to interface functions. The TLEA must identify the other party (service provider), where applicable, that will manage access on its behalf to the NaTIS.

The Corporation shall require the TLEA to attach a copy of the Service Level Agreement with the other party.

Suitable network access connectivity shall be determined by the Corporation in terms of the Network Standard for Direct Access.

B: Non-designated entities

These are the entities and individuals that request access to Road Traffic Information and use it for various reasons.

Provision of Road Traffic Information to these users is by means of a system-to-system interface or data extraction according to the RTI user's requirements.

An entity requiring access to NaTIS Information shall apply in the prescribed format, on an ANI form, to the Access to NaTIS Information (ANI) workgroup, for access to NaTIS Information.

The Access to NaTIS Information (ANI) workgroup, shall at its next ordinary sitting, consider the applications received guided by the principles outlined in the General Principles section.

3.2.6 FINANCIAL SERVICES

- Bid evaluation reports
- Bid Committee's minutes or recordings
- Evaluation Scoresheets
- Deviations from normal procurement processes
- Acquisition related procurement documents
- Contracts
- Quarterly Financial Statements Fruitless expenditure report
- Irregular expenditure report

3.2.7 CORPORATE SERVICES

a) Training Norms and Standards Unit

- Enrolment details of trainees for Authorised Officers' courses as Traffic Training Centres
- Assessment request for Authorised Officer's Courses from Traffic Training Centres
- Moderation and Traffic College Evaluation Reports

(b) Human Capital

- Employee Records
- Job Applicants Records

(c) Legal and Compliance Services

- Legal Opinions
- Litigation Papers
- Internal Reports
- Correspondence between attorney and client containing communications of a confidential and privileged nature, with the object of obtaining legal advice in relation to the matter in question in this action, prior to, in contemplation of, and during the continuation of these proceedings.
- Statements of witnesses and reports or tape recordings brought into existence prior to, in contemplation of, and during the continuation of these proceedings, and correspondence and documents and tape recordings in relation to the evidence to be used in relation to information or otherwise to enable the Defendant's case in this action to be conducted, which statements, reports, correspondence and documents and tape recordings are by their nature legally privileged.
- Instructions to counsel, cases for the opinion of counsel, notes and opinions thereon with counsel's advice and drafts of documents given upon such instruction and briefs to counsel, which came into existence prior to, in contemplation of, and during the continuation of these proceedings, solely for the purpose of obtaining for, or furnishing the Defendant's or Defendant's attorneys, legal advice in relation to these proceedings or which may have been confidential in relation to the matter in question in this action, which documents are by their nature legally privileged.
- All file notes and memoranda which are of a privileged nature.
- All documents and correspondence which are by their nature legally privileged in respect of these proceedings between the parties

(d) Total Facilities Management

- Internal submissions, memorandums and communication
- Internal Reports

- Fleet and Asset Register

(e) Operational Secretariat Services

- Internal Memorandums
- Internal Meeting Minutes
- Attendance Records

3.3 TRANSBORDER FLOWS OF PERSONAL INFORMATION

Section 72 of POPIA regulates the transfer of personal information outside the Republic. In compliance with this provision, the RTMC will not transfer personal information about a data subject to a third party who is in a foreign country unless any one of the following conditions/considerations exists:

- i. The Third Party is a Department or Agency of a foreign government and there exists a Memorandum Of Understanding (MOU) to exchange information between the Ministry of Transport of the Republic and the Foreign government;
- ii. The Third Party, who is the recipient of the information, is subject to a law, binding corporate rules or binding agreement which provides an adequate level of protection that reflect the principles of POPIA;
- iii. The data subject consents to the transfer;
- iv. The transfer is necessary for the performance of a contract between the data subject and the responsible party;
- v. The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject; or the transfer is for the benefit of the data subject.

3.4 SAFEGUARDING OF INFORMATION HELD BY THE RTMC

- 3.4.1 The RTMC takes extensive information security measures to ensure the Confidentiality, Integrity and Availability of personal information in its possession.

3.4.2 The RTMC takes appropriate technical and organisational measures designed to ensure that personal data remains confidential and secure against unauthorised or unlawful processing and against accidental loss, destruction or damage.

3.5 INFORMATION REGULATOR'S GUIDE ON HOW TO USE POPIA and PAIA

3.5.1 The Information Regulator (which has replaced the South African Human Rights Commission) is an independent body established in terms of section 39 of POPI and is subject only to the law and the Constitution, being accountable to the National Assembly.

3.5.2 The Information Regulator is, among others, empowered to monitor and enforce compliance by public and private bodies with the provisions of POPI and PAIA

3.5.3 The Information Regulator will in due course update and make available the existing guide that has been compiled by the South African Human Rights Commission containing such information, in an easily comprehensible form and manner, as may reasonably be required by a person who wishes to exercise any right contemplated in PAIA and POPI.

3.5.4 Any enquiries in respect of personal information should be directed to:

The Information Regulator

Contact Details:

Tel: 012 406 4818

Fax: 086 500 3351

Email: infoereg@justice.gov.za

3.6 PAIA MANUAL

As provided for in terms of PAIA, this manual will be updated as and when the need arises and as soon as any amendments have been finalised. The latest version of this manual will be made public through:

- a) The RTMC's Website www.rtmc.co.za
- b) Head Office of the RTMC for public inspection during normal business hours; and
- c) The request of any person upon the payment of applicable fees.
- d) Press Releases.

3.7 ACCESS TO INFORMATION HELD BY THE RTMC UNDER PAIA and POPIA

In terms of section 11 of PAIA, a person must be given access to a record of the RTMC if the person complies with all the procedural requirements in PAIA relating to a request for access to that record; and access to that record is not refused in terms of any ground for refusal contemplated in PAIA.

POPIA, in section 23, provides that a person, upon proof of identity, may request the RTMC to confirm, free of charge, all the information it holds about the data subject and may request access to such information, including information about the identity of Third Parties who have or have had access to such information

Where the person is required to pay a fee for services provided to him/her/it, the RTMC must provide the person with a written estimate of the amount payable before providing the information and may require that the person pay a deposit for all or part of the fee.

3.8 INFORMATION REQUEST PROCEDURES

Persons requesting access to information held by the RTMC in terms of:

- a. PAIA must use **Form 2** attached to this guide;
- b. POPIA must use the form to be prescribed in terms of the POPI Regulations.

The request for information must be made on the prescribed form to the Information Officer of RTMC whose details are provided in section 6.12.1 below. The requester must specify the following in the request:

- a. The record requested;
- b. The personal particulars of the requester including contact numbers in the Republic of South Africa;
- c. The language in which such record is requested (note that if the record is not available in the language the requester prefers, access may be granted in the language in which the record is available);
- d. Capacity in which the requester is requesting the information;
- e. Form of access required;
- f. Reasons for the request.

Should a requester require the assistance of the Information Officer in obtaining any record held by the RTMC, such assistance will be provided by the Information Officer or his/her Deputy. The record

requested will be furnished on payment of the prescribed fee. A deposit may be requested from the requester in respect of the access fee.


3.9 PRESCRIBED FEES

The fees have been prescribed in the Regulations promulgated in terms of PAIA and must be paid by a requester before the RTMC contact persons can make any records requested available to the requester.

Non-PAIA fees apply where information requested has no bearing on the rights or protection of the requester. RTMC has publish these fees under Section 24 read with Section 48 of the Road Traffic Management Act no 20 of 1999 from time to time.

Payment of fees can be made via a direct deposit into the account of the RTMC. Details of the RTMC's account can be requested from the Deputy Information Officer. Proof of payment must be supplied before a request is processed. Such proof - clearly indicated as payment for the request concerned - must be delivered or posted by registered mail to the Deputy Information Officer.

3.10 CONTACT DETAILS OF INFORMATION OFFICER AND DEPUTY INFORMATION OFFICERS

 ROAD TRAFFIC MANAGEMENT CORPORATION				
Officer	Name	Address	Contact number	Mail
Information Officer	Adv Makhosini Msibi Chief Executive Officer	Centurion Gate Business Park, Block A To D, 146 Akkerboom Street, Zwartkop, Centurion, 0157 Gauteng, South Africa	Tel: 012 999-5200 Alternative Tel: 087 310-8200	Info@rtmc.co.za
Deputy Information Officer	Ms Thenjiwe Mjoli GM: TFM	Centurion Gate Business Park, Block A To D, 146 Akkerboom Street, Zwartkop, Centurion, 0157 Gauteng, South Africa	Tel: 012 999-5200 Alternative Tel: 012 999-5365	paia@rtmc.co.za or Thenjiwe.Mjoli@rtmc.co.za

3.11 Time Limits

Upon receipt of the request, where applicable, the Information Officer or Deputy Information Officer will inform any Third Party affected within 30 days of receipt of the request. The Third Party must inform the Information Officer or Deputy Information Officer why such information should not be made available to the requester.

The decision whether or not to grant the request will be made by the Information Officer within 45 days of receipt of the request. This period may be extended once for an additional period of 30 days.

4. GROUNDS FOR REFUSAL

The Information Officer may refuse a request for information for the following reasons:

- a) Where the disclosure would amount to an unreasonable disclosure of personal information;
- b) Where the disclosure would amount to disclosure of the trade secrets of a third party;
- c) Where the disclosure would lead to a revelation of financial, commercial, scientific or technical information of a third party;
- d) Where such information was supplied in confidence by a third party;
- e) Where the disclosure would breach the duty of confidence owed to a third party;
- f) Where the disclosure would endanger the life or physical safety of an individual;
- g) If the disclosure is prohibited under the Criminal Procedure Act;
- h) If the disclosure is privileged under legal proceedings or research conducted by or on behalf of a third party;
- i) Where the disclosure would compromise the investigation where proceedings are pending.

5. PROCEDURE FOR LODGING AN INTERNAL APPEAL

- a) A party aggrieved by the decision of the Information Officer in refusing the request may lodge an internal appeal with the relevant authority within 60 days of the decision. The relevant authority shall be the Chief Executive Officer.
- b) The appeal must be lodged on the prescribed form and sent to the Information Officer of the RTMC at the address indicated above. The appeal must state the reasons for the internal appeal and any other relevant information known to the appellant.
- c) A party wishing to lodge the appeal must pay the prescribed fee.
- d) On receipt of the internal appeal, the Information Officer must submit to the relevant authority, the internal appeal together with his/her reasons for the decision and if the internal appeal is as a result of the refusal of granting of a request for access, the name, postal address, phone, fax number and an electronic mail address of any Third Party that must be notified of the request.
- e) The relevant authority considering the appeal must inform the Third Party to whom the record relates of the internal appeal. This must be done within 30 days after receipt of the internal appeal. The Third Party must be given an opportunity to make representations within 21 days of being informed of the appeal.
- f) When making a decision, the Chief Executive Officer/Registrar may confirm the decision appealed against or substitute it with a new decision. The internal appeal must be decided upon within 30 days after the Information Officer has received the notice of internal appeal.

- g) Once a decision has been made, notice must be given to the appellant and to every Third Party who was informed and to the requester. The notice must state adequate reasons for the decision, including the provisions of the Act relied upon and advise the appellant that he/she may lodge an application with the court against the decision of the internal appeal within 60 days.

6. APPLICATION TO COURT

- a) A requester or Third Party may only apply to a court for appropriate relief in terms of section 82 of PAIA after that requester or Third Party has exhausted the internal appeal procedure against a decision of the information officer of the RTMC provided for in section 74 of the aforementioned Act.
- b) A requester that has been unsuccessful in an internal appeal to the relevant authority of the RTMC; aggrieved by a decision of the relevant authority of the RTMC to disallow the late lodging of an internal appeal in terms of section 75(2); aggrieved by a decision of the information officer of the RTMC to refuse a request for access; or taken in terms of section 22, 26 (1) or 29 (3) may, by way of an application within 180 days, apply to a court for appropriate relief in terms of section 82.

FORM 2: REQUEST FOR ACCESS TO RECORD

[Regulation 7]

NOTE:

1. Proof of identity must be attached by the requester.
2. If requests made on behalf of another person, proof of such authorisation, must be attached to this form.

TO: The Information Officer

 (Address)

E-mail address: _____

Fax number: _____

Mark with an "X"

- Request is made in my own name Request is made on behalf of another person.

PERSONAL INFORMATION			
Full Names			
Identity Number			
Capacity in which request is made <i>(when made on behalf of another person)</i>			
Postal Address			
Street Address			
E-mail Address			
Contact Numbers	Tel. (B):		Facsimile:
	Cellular:		
Full names of person on whose behalf request is made <i>(if applicable)</i> :			
Identity Number			
Postal Address			

Street Address			
E-mail Address			
Contact Numbers	Tel. (B)		Facsimile
	Cellular		
PARTICULARS OF RECORD REQUESTED			
<p><i>Provide full particulars of the record to which access is requested, including the reference number if that is known to you, to enable the record to be located. (If the provided space is inadequate, please continue on a separate page and attach it to this form. All additional pages must be signed.)</i></p>			
Description of record or relevant part of the record:			
Reference number, if available			
Any further particulars of record			
TYPE OF RECORD <i>(Mark the applicable box with an "X")</i>			
Record is in written or printed form			
Record comprises virtual images <i>(this includes photographs, slides, video recordings, computer-generated images, sketches, etc)</i>			
Record consists of recorded words or information which can be reproduced in sound			
Record is held on a computer or in an electronic, or machine-readable form			

FORM OF ACCESS <i>(Mark the applicable box with an "X")</i>	
Printed copy of record <i>(including copies of any virtual images, transcriptions and information held on computer or in an electronic or machine-readable form)</i>	
Written or printed transcription of virtual images <i>(this includes photographs, slides, video recordings, computer-generated images, sketches, etc)</i>	
Transcription of soundtrack <i>(written or printed document)</i>	
Copy of record on flash drive <i>(including virtual images and soundtracks)</i>	
Copy of record on compact disc drive <i>(including virtual images and soundtracks)</i>	
Copy of record saved on cloud storage server	

MANNER OF ACCESS <i>(Mark the applicable box with an "X")</i>	
Personal inspection of record at registered address of public/private body <i>(including listening to recorded words, information which can be reproduced in sound, or information held on computer or in an electronic or machine-readable form)</i>	
Postal services to postal address	
Postal services to street address	
Courier service to street address	
Facsimile of information in written or printed format <i>(including transcriptions)</i>	
E-mail of information <i>(including soundtracks if possible)</i>	
Cloud share/file transfer	
Preferred language <i>(Note that if the record is not available in the language you prefer, access may be granted in the language in which the record is available)</i>	

PARTICULARS OF RIGHT TO BE EXERCISED OR PROTECTED	
<i>If the provided space is inadequate, please continue on a separate page and attach it to this Form. The requester must sign all the additional pages.</i>	
Indicate which right is to be exercised or protected	

Explain why the record requested is required for the exercise or protection of the aforementioned right:	

FEES	
a)	<i>A request fee must be paid before the request will be considered.</i>
b)	<i>You will be notified of the amount of the access fee to be paid.</i>
c)	<i>The fee payable for access to a record depends on the form in which access is required and the reasonable time required to search for and prepare a record.</i>
d)	<i>If you qualify for exemption of the payment of any fee, please state the reason for exemption</i>
Reason	

You will be notified in writing whether your request has been approved or denied and if approved the costs relating to your request, if any. Please indicate your preferred manner of correspondence:

Postal address	Facsimile	Electronic communication <i>(Please specify)</i>

Signed at _____ this _____ day of _____ 20 _____

Signature of Requester / person on whose behalf request is made

FOR OFFICIAL USE

Reference number:	
Request received by: <i>(State Rank, Name And Surname of Information Officer)</i>	
Date received:	
Access fees:	
Deposit (if any):	

Signature of Information Officer