No 265 of 2009 published in *Gazette 5.11.2009 p 5109*

South Australia

# Road Traffic (Intelligent Access Program) Regulations 2009

under the *Road Traffic Act 1961*

## Contents

# Part 1—Preliminary

## 1—Short title

These regulations may be cited as the *Road Traffic (Intelligent Access Program) Regulations 2009*.

## 2—Commencement

These regulations will come into operation on 1 May 2010.

## 3—Interpretation

(1) In these regulations—

***Act*** means the *Road Traffic Act 1961*;

***approved intelligent transport system*** means an intelligent transport system approved for the purposes of the IAP by TCA;

***compliance purposes*** has the same meaning as in section 40F of the Act;

***IAP*** is the acronym for *Intelligent Access Program*;

***IAP agreement*** means an agreement between the operator of a vehicle and an IAP service provider under which the IAP service provider agrees to provide IAP monitoring services to the operator;

***IAP audit***—see regulation 34;

***IAP auditor*** means a person approved as an IAP auditor by TCA;

***IAP condition***—see regulation 6;

***IAP information*** means information that has been generated or collected for any purpose relating to the IAP;

***IAP service provider*** means a person that is certified as an IAP service provider by TCA;

***IAP vehicle*** means a vehicle that is subject to an IAP condition, is equipped for monitoring under the IAP, and is covered by an IAP agreement;

***intelligent access map*** means the spatial data set, issued by TCA from time to time, that defines the national public road system;

***Intelligent Access Program***—see regulation 4;

***law-enforcement purposes*** means the purposes of investigating or prosecuting an offence (whether summary or indictable) against—

(a) a road law; or

(b) a corresponding road law; or

(c) a law relating to the transport by road of dangerous goods;

***malfunction*** of an approved intelligent transport system—see subregulation (4);

***non-compliance report***—see subregulation (2);

***participating operator*** means an operator of a vehicle or vehicles that has entered into an IAP agreement, and operates at least 1 IAP vehicle;

***personal information*** means information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion;

***tampering*** with an approved intelligent transport system—see regulation 44;

***TCA*** means Transport Certification Australia Ltd ACN 113 379 936.

(2) A ***non-compliance report***—

(a) is a report, generated by an approved intelligent transport system, of a contravention by an IAP vehicle of an IAP condition; and

(b) may include information, about apparent tampering with that system, electronically generated by the system itself.

(3) A reference in a provision of these regulations to an approved form is a reference to the form approved by the Authority for the purposes of the provision.

(4) An approved intelligent transport system ***malfunctions*** if—

(a) it ceases to work at all, or works only intermittently; or

(b) it does not perform 1 or more functions required under the IAP, or performs any such function only intermittently; or

(c) it performs such a function in such a way that the results of its doing so are inaccurate or unreliable (including intermittently inaccurate or unreliable).

### 4—What the Intelligent Access Program is

The Intelligent Access Program is a program to allow heavy vehicles to have access, or improved access, to the road network in return for monitoring, by an intelligent transport system, of their compliance with specified access conditions.

### 5—Other means of enforcement not excluded

Nothing in these regulations has the effect of preventing or excluding any other method of enforcement of a road law.

## Part 2—Powers and duties of Authority in relation to IAP

### 6—What IAP conditions do

(1) In this regulation—

***IAP road*** means a road or road-related area specified in an IAP condition for use by IAP vehicles.

(2) An ***IAP condition*** is the specification of the conditions in relation to the IAP under which IAP vehicles are allowed to be used on an IAP road.

(3) An IAP condition—

(a) must specify at least 1 IAP road (***spatial data***); and

(b) may specify—

(i) periods during which IAP vehicles are permitted to use the specified IAP road (***temporal data***); and

(ii) maximum speeds at which IAP vehicles may travel during that use (***speed data***); and

(iii) any other condition of access to the IAP road (for example, a condition about mass limits); and

(c) may specify a period within which an approved intelligent transport system must generate, and send to the Authority, a non-compliance report after the system detects a non-compliance with the condition by an IAP vehicle.

(4) If an IAP condition does not specify speed data, it is taken to authorise the use of IAP vehicles on the IAP road at any speed at which a non-IAP vehicle of the same class could be used on the IAP road.

(5) An IAP condition that specifies speed data does not authorise an IAP vehicle to travel at a speed in excess of a speed limit that applies to vehicles generally.

(6) If an IAP condition does not specify temporal data, it is taken to authorise the use of IAP vehicles on the IAP road at any time at which a non-IAP vehicle of the same class could be used on the IAP road.

(7) An IAP condition may require an IAP vehicle to be monitored whether or not it uses an IAP road.

### 7—Authority may specify IAP conditions

(1) The Authority may specify IAP conditions.

(2) The Authority may combine an IAP condition with a mass, dimension or load restraint concession.

(3) An IAP condition not combined with such a concession must be published by notice in the Gazette.

### 8—Issue of IAP identifiers

(1) The Authority may issue an IAP identifier for an IAP vehicle.

(2) If an IAP identifier is, or becomes, known to a person or entity that has the ability to associate it with a particular individual, the person or entity must treat the identifier as personal information for the purposes of a law relating to privacy.

## Part 3—Duties and obligations etc of operators of vehicles

### 9—Offence—providing false or misleading information to IAP service provider

(1) The operator of an IAP vehicle commits an offence if—

(a) the operator gives information to an IAP service provider with which the operator has entered into an IAP agreement; and

(b) the information is relevant to the operation of the vehicle; and

(c) the information—

(i) is false or misleading; or

(ii) omits anything without which the information is false or misleading.

Maximum penalty: $10 000.

(2) Subregulation (1) does not apply because of subregulation (1)(c)(i) if the information was not false or misleading in a material particular.

(3) Subregulation (1) does not apply because of subregulation (1)(c)(ii) if the information omitted did not render the information given false or misleading in a material particular.

(4) Without limiting subregulation (1)(b), information about an IAP condition that applies, or is capable of applying, to a vehicle is relevant to the operation of the vehicle.

(5) The operator of a vehicle commits an offence if—

(a) the operator gives information to an IAP service provider; and

(b) the operator intends that the IAP service provider will enter into an IAP agreement with the operator in reliance on the information; and

(c) the information—

(i) is false or misleading; or

(ii) omits anything without which the information is false or misleading.

Maximum penalty: $10 000.

(6) Subregulation (5) does not apply because of subregulation (5)(c)(i) if the information was not false or misleading in a material particular.

(7) Subregulation (5) does not apply because of subregulation (5)(c)(ii) if the information omitted did not render the information given false or misleading in a material particular.

## 10—Operators' obligation to tell drivers about collection of personal information and other matters

(1) The operator of an IAP vehicle must take reasonable steps to tell the vehicle's driver, before the vehicle begins a journey—

(a) that the vehicle will be monitored by an IAP service provider; and

(b) what information will be collected by the IAP service provider; and

(c) the purposes for which that information is collected; and

(d) the persons and authorities to which information so collected may be disclosed; and

(e) that the collection of the information is authorised by these regulations; and

(f) that the driver has the rights of reasonable access to, and of correction of, personal information so collected, and how those rights can be exercised; and

(g) the name and address of the IAP service provider.

Maximum penalty: $10 000.

(2) The operator of an IAP vehicle must take reasonable steps to tell the vehicle's driver, before the vehicle begins a journey—

(a) about the driver's obligation under regulation 13; and

(b) how the driver can make the reports required by that obligation.

Maximum penalty: $10 000.

(3) An operator may comply with subregulation (1) and (2) by—

(a) placing a notice that gives the required information in a place in the vehicle's driving cab where it is clearly visible; or

(b) giving the required information to the driver in writing as part of a written contract of employment between the driver and the operator.

### 11—System malfunctions—duties of operators of IAP vehicles

(1) If the operator of an IAP vehicle becomes aware that an approved intelligent transport system fitted to the vehicle is malfunctioning, the operator must tell the Authority about the malfunction immediately, in person or by radio, telephone, fax or email.

Maximum penalty: $5 000.

(2) The operator of such a vehicle must keep a written record of reports of such malfunctions, including—

(a) the date, time and type of the malfunction, and the location of the vehicle concerned at the time of the malfunction; and

(b) the date, time, location of the vehicle, type of report, who made the report and who the report was made to.

Maximum penalty: $5 000.

### 12—Offence—breach of IAP conditions

(1) The operator of an IAP vehicle commits an offence if a driver of the vehicle, or any other person, breaches an IAP condition applying in relation to the vehicle.

Maximum penalty: $10 000.

(2) Subregulation (1) applies in relation to—

(a) a breach of an IAP condition in this State; or

(b) a breach of an IAP condition in another jurisdiction if the journey of the vehicle during which the breach occurs resulted from action taken by the person as the operator of the vehicle in this State.

(3) A person charged has the benefit of the reasonable steps defence for an offence against this regulation.

(4) It is a defence to a charge for an offence against this regulation if the person charged establishes that the vehicle was being used at the relevant time by—

(a) another person not entitled (whether by express or implied authority or otherwise) to use it, other than an employee or agent of the person; or

(b) by an employee of the person who was acting at the relevant time outside the scope of the employment; or

(c) by an agent of the person who was acting at the relevant time outside the scope of the agency.

## Part 4—Duties of vehicle drivers

### 13—System malfunctions—drivers' duties

(1) If the driver of an IAP vehicle becomes aware that an approved intelligent transport system fitted to the vehicle is malfunctioning, the driver must tell the vehicle's operator about the malfunction immediately, in person or by radio, telephone, fax or email.

Maximum penalty: $5 000.

(2) The driver of such a vehicle must keep a written record of such reports, including—

(a) the date, time and type of the malfunction, and the location of the vehicle concerned at the time of the malfunction; and

(b) the date and time of the malfunction, the location of the vehicle at the time, the type of report, who made the report and who the report was made to.

Maximum penalty: $5 000.

# Part 5—Duties, powers and obligations of IAP service providers

## 14—IAP service providers' duties in regard to use and disclosure of information

An IAP service provider must not use or disclose IAP information otherwise than as required or authorised by these regulations or any other law.

Maximum penalty:

(a) for a first offence—$10 000;

(b) for a second or subsequent offence—$20 000.

## 15—IAP service providers' powers to collect, store, use and disclose IAP information

(1) An IAP service provider may collect, store and use IAP information (including personal information) for compliance purposes.

(2) An IAP service provider may disclose IAP information (including personal information) to the Authority, or to TCA, for compliance purposes.

(3) An IAP service provider may disclose IAP information (including personal information, but not including a non-compliance report or a report under regulation 21) to a police officer, or to an authorised officer, for law enforcement purposes if so authorised by a warrant issued by a court.

(4) If an IAP service provider discloses IAP information to a police officer or an authorised officer under subregulation (3), the police officer or authorised officer must not use the information, or disclose it to any other person, unless—

(a) the police officer or authorised officer believes the use or disclosure is reasonably necessary for law-enforcement purposes; or

(b) the use or disclosure is otherwise authorised by these regulations.

(5) With the consent of a participating operator, an IAP service provider may use or disclose IAP information about the operator to a person other than the operator for any purpose if the information—

(a) does not identify any individual; and

(b) contains nothing by which the identity of any individual can reasonably be ascertained.

(6) An IAP service provider may disclose IAP information (except a non-compliance report) about a participating operator to the operator.

(7) In addition, an IAP service provider may use or disclose IAP information (including personal information)—

(a) with the consent of any person about whom the IAP information includes personal information; or

(b) as otherwise authorised by these regulations or any other law.

(8) An IAP service provider must give an IAP auditor access to any record kept by the IAP service provider for the purposes of these regulations.

## 16—IAP service providers' duties in regard to recording use and disclosure of information

(1) If an IAP service provider uses or discloses IAP information, the IAP service provider must make a record of the use or disclosure containing the following information:

(a) the name of the person who used or disclosed the IAP information;

(b) the date of the disclosure or use;

(c) in the case of a disclosure of IAP information, the person or body to whom or to which that information was disclosed;

(d) in the case of the use of IAP information by the IAP service provider, a brief description of how the information was used;

(e) what provision of these regulations or another law the disclosure or use was authorised by;

(f) if the authority for the disclosure or use also required a document (for example, a warrant, a certificate or a consent), a copy of the document.

(2) The IAP service provider must make the record within 5 business days after the relevant use or disclosure.

(3) The IAP service provider must make the record in a form that allows the record to be readily inspected.

(4) The IAP service provider must retain the record for 2 years.

(5) An IAP service provider commits an offence if it does not comply with a requirement of any of subregulations (1) to (4).

Maximum penalty:

(a) for a first offence—$10 000;

(b) for a second or subsequent offence—$20 000.

## 17—IAP service providers' obligations in regard to quality and security of IAP information

(1) An IAP service provider must take reasonable steps to ensure that the IAP information it collects—

(a) is necessary for, or is directly related to, the purpose for which it is collected, or a directly related purpose; and

(b) is not excessive for that purpose; and

(c) is accurate, up-to-date and complete.

Maximum penalty: $5 000.

(2) An IAP service provider must take reasonable steps to ensure that the collection of IAP information does not intrude to an unreasonable extent on the personal privacy of any individual to whom the information relates.

(3) If an individual (including an individual who is a participating operator) about whom an IAP service provider holds personal information so requests, an IAP service provider must make appropriate alterations to the personal information to ensure that the information is accurate, complete, up-to-date and not misleading.

(4) If the IAP service provider considers that the personal information the subject of such a request is not inaccurate, incomplete, out-of-date or misleading, it may refuse to comply with the request, but must then—

(a) give the individual a statement in writing of its reasons for refusing; and

(b) if the individual so requests, attach to, or include with, the information a statement by him or her.

## 18—IAP service providers' obligations to keep records of monitoring

(1) An IAP service provider must keep a record of the IAP information that it collects.

(2) The record must be organised in a way that allows the record to be conveniently and properly audited.

(3) An IAP service provider must keep—

(a) a copy of a non-compliance report; and

(b) the data that were relied on to generate the report,

for at least 4 years after the report is made by the provider.

Maximum penalty: $10 000.

(4) An IAP service provider must take reasonable steps to protect IAP information collected by it against unauthorised access, unauthorised use, misuse, loss, modification or unauthorised disclosure.

(5) An IAP service provider must take reasonable steps to destroy IAP information (including personal information), other than information required by subregulation (3) to be kept, 1 year after the information is collected.

Maximum penalty: $10 000.

## 19—IAP service providers' obligation to make individuals aware of personal information held

(1) An IAP service provider must prepare, and make publicly available, a document that sets out its policies on the management of information.

(2) If an individual about whom an IAP service provider holds personal information so requests, the IAP service provider must, subject to subregulation (4), take reasonable steps to inform him or her of—

(a) the kinds of information it holds about him or her; and

(b) the purpose for which the information is held; and

(c) the way in which it collects, holds, uses and discloses the information; and

(d) the persons and authorities to whom or to which the information may be disclosed; and

(e) that he or she has the rights of reasonable access to, and of correction of, the information; and

(f) how to exercise those rights.

(3) Subject to subregulation (4), an IAP service provider must, on request by an individual about whom the IAP service provider holds personal information, give him or her access to the information, and must do so without undue delay or cost.

(4) However, nothing in subregulation (2) or (3) requires an IAP service provider—

(a) to inform an individual that a report under regulation 20 or 21 exists or has been made; or

(b) to give an individual access to such a report.

Maximum penalty: $10 000.

## 20—IAP service providers' obligation to make non-compliance reports

(1) For the purposes of this regulation, an IAP service provider is taken to know of a breach of an IAP condition if the IAP service provider's monitoring equipment has detected the breach.

(2) An IAP service provider commits an offence if the IAP service provider—

(a) knows of—

(i) a breach by a participating operator of an IAP condition; or

(ii) anything that indicates that a participating operator may have breached such a condition; and

(b) does not make a non-compliance report that complies with subregulation (3) to the Authority within the time allowed, in the circumstances, under subregulation (4).

Maximum penalty:

(a) for a first offence—$10 000;

(b) for a second or subsequent offence—$20 000.

(3) A non-compliance report must be in the form approved for the purpose by TCA, and must contain any information required by the IAP service provider's certification.

(4) The IAP service provider must make the report—

(a) within any time specified in the relevant IAP condition; or

(b) within any time specified by the Authority (by written direction) for the purpose.

## 21—IAP service providers' obligation to report tampering

(1) In this regulation, a reference to knowledge or suspicion does not include knowledge or suspicion resulting only from—

(a) a report, contained in a non-compliance report or otherwise made by an approved intelligent transport system, of the electronic detection of apparent tampering with that system; or

(b) the analysis of data produced by such a system.

(2) An IAP service provider commits an offence if the IAP service provider—

(a) either—

(i) knows that intelligent transport system equipment has been tampered with; or

(ii) has reasonable grounds to suspect that intelligent transport system equipment has been tampered with; and

(b) does not report, in accordance with subregulation (3), to the Authority within 5 business days.

Maximum penalty:

(a) for a first offence—$10 000;

(b) for a second or subsequent offence—$20 000.

(3) The report must be in the form approved by TCA for the purpose, and must contain any information required by the IAP service provider's certification.

(4) If an IAP service provider knows, or has reasonable grounds to suspect, that approved intelligent transport system equipment has been tampered with, the IAP service provider must not disclose to any person other than the Authority—

(a) that the provider has that knowledge or suspicion; or

(b) any information from which the person to whom the disclosure is made could reasonably infer that the provider had that knowledge or suspicion.

Maximum penalty:

(a) for a first offence—$10 000;

(b) for a second or subsequent offence—$20 000.

(5) If an IAP service provider has made a report to the Authority under subregulation (2) or (3) of apparent tampering or suspicion of tampering, the provider must not disclose to any person other than the Authority—

(a) that the report has been made; or

(b) any information from which the person to whom the disclosure is made could reasonably infer that the provider had made such a report.

Maximum penalty:

(a) for a first offence—$10 000;

(b) for a second or subsequent offence—$20 000.

## 22—Offence—IAP service provider providing false or misleading information to Authority or TCA

(1) An IAP service provider commits an offence if—

(a) the IAP service provider gives information to the Authority or TCA; and

(b) the information is relevant to the operation of an IAP vehicle; and

(c) the information—

(i) is false or misleading; or

(ii) omits anything without which the information is false or misleading.

Maximum penalty: $10 000.

(2) Subregulation (1) does not apply because of subregulation (1)(c)(i) if the information was not false or misleading in a material particular.

(3) Subregulation (1) does not apply because of subregulation (1)(c)(ii) if the information omitted did not render the information given false or misleading in a material particular.

## 23—Functions of TCA

For the purposes of these regulations, the functions of TCA are—

(a) to manage the certification and audit regime for the Intelligent Access Program; and

(b) to certify and audit, and cancel the certification of, IAP service providers; and

(c) to appoint and coordinate IAP auditors.

## 24—TCA's duties in regard to use and disclosure of information

(1) TCA must not use or disclose IAP information unless it first takes reasonable steps to ensure that, having regard to the purpose for which the information is to be used or disclosed, that the information is accurate, complete, up-to-date and not misleading.

(2) Subject to regulations 26 and 27, TCA must not use or disclose information for a purpose other than the purpose for which the information was collected.

(3) TCA must not use or disclose information relating to a particular participating operator other than to—

(a) the operator; or

(b) an IAP auditor; or

(c) the Authority,

unless the disclosure is authorised under these regulations or another law.

(4) TCA must not disclose information relating to a breach of an IAP service provider's obligations except to—

(a) the Authority; or

(b) an IAP auditor.

(5) If TCA uses or discloses IAP information (other than use or disclosure for law enforcement), TCA must make a record of the use or disclosure containing the following information:

(a) the name of the person who used or disclosed the IAP information;

(b) the date of the disclosure or use;

(c) in the case of a disclosure of IAP information, the person or body to whom or to which the information was disclosed;

(d) in the case of the use of IAP information by TCA, a brief description of how the information was used;

(e) what provision of these regulations or another law the disclosure or use was authorised by;

(f) if the authority for the disclosure or use also required a document (for example, a warrant, a certificate or a consent), a copy of the document.

(6) TCA must make the record within 5 business days after the relevant use or disclosure.

(7) TCA must make the record in a form that allows the record to be readily inspected.

(8) TCA must retain the record for 2 years.

## 25—TCA's powers to collect, store, use and disclose IAP information

(1) TCA may collect, store, use and disclose IAP information (including personal information) for the performance of its functions and for law enforcement purposes.

(2) With the consent of a participating operator, TCA may use or disclose IAP information about the operator for any purpose if the information—

(a) does not identify any individual; and

(b) contains nothing by which the identity of any individual can reasonably be ascertained.

(3) TCA may use or disclose IAP information (including personal information)—

(a) with the consent of any person about whom the IAP information includes personal information; or

(b) as otherwise authorised by these regulations or any other law.

## 26—Disclosure of information for law-enforcement purposes etc

(1) TCA may disclose IAP information (including personal information but not including a non-compliance report or a report under regulation 21) to a nominated police officer or an authorised officer for law-enforcement purposes if so authorised by a warrant issued by a court.

(2) If TCA discloses information to a police officer or an authorised officer under subregulation (1), the police officer or authorised officer must not use that information, or disclose the information to any other person unless—

(a) the police officer or authorised officer believes the use or disclosure is reasonably necessary for law-enforcement purposes; or

(b) the use or disclosure is otherwise authorised under these regulations.

## 27—Use of information for research

TCA may use or disclose information for research purposes, but only if the information contains no personal information.

## 28—TCA's obligations in regard to collecting IAP information

(1) TCA must take reasonable steps to ensure that IAP information that it collects—

(a) is necessary for, or is directly related to, the purpose for which it is collected, or a directly related purpose; and

(b) is not excessive for that purpose; and

(c) is accurate, up-to-date and complete.

(2) TCA must take reasonable steps to ensure that the collection of IAP information does not intrude to an unreasonable extent on the personal privacy of any individual to whom the information relates.

## 29—TCA's obligation to keep information secure

(1) TCA must take reasonable steps to protect IAP information collected by it against unauthorised access, unauthorised use, misuse, loss, modification or unauthorised disclosure.

(2) TCA must take reasonable steps to destroy IAP information (including personal information) after 1 year unless the information is required as evidence.

(3) TCA may comply with subregulation (2) by permanently removing anything by which an individual can be identified from the IAP information that it holds.

## 30—TCA's obligation to make individuals aware of personal information held

(1) TCA must prepare, and make publicly available, a document that sets out its policies on the management of information.

(2) If an individual so requests, TCA must take reasonable steps to inform him or her of—

(a) the kinds of information it holds about him or her; and

(b) the purpose for which the information is held; and

(c) the way in which it collects, holds, uses and discloses the information; and

(d) the persons and authorities to whom or to which the information may be disclosed; and

(e) that the collection of the information is authorised by these regulations; and

(f) that he or she has the rights of reasonable access to, and of correction of, the information, and how those rights can be exercised.

(3) TCA must, on request by an individual about whom TCA holds personal information, give him or her access to the information, and must do so without undue delay or cost.

(4) With the consent of a participating operator, TCA may use or disclose IAP information about the operator for any purpose if the information—

(a) does not identify any individual; and

(b) contains nothing by which the identity of any individual can reasonably be ascertained.

## 31—TCA's obligation to keep records of transactions

(1) TCA must keep and retain records, in accordance with this regulation, of its transactions with the Authority, IAP service providers and IAP auditors.

(2) The records must be organised in such a way as will enable them to be conveniently and properly audited.

(3) TCA must keep a non-compliance report for at least 4 years after its receipt.

(4) TCA must retain any other record referred to in subregulation (1) for at least 1 year after the record is made.

## 32—TCA's obligation to correct errors etc

(1) TCA must take reasonable steps to ensure that personal information that it collects is accurate, complete, up-to-date and not misleading.

(2) If so requested by a participating operator or an IAP service provider, TCA must make appropriate alterations to any personal information it holds to ensure that the information is accurate, complete, up-to-date and not misleading.

(3) If TCA considers that the personal information the subject of such a request is not inaccurate, incomplete, out-of-date or misleading, it may refuse to comply with the request, but must then—

(a) give the operator or provider a written statement of its reasons for refusing; and

(b) if the operator or provider so requests, attach to, or include with, the information a statement by the operator or provider.

## 33—TCA's obligation to report tampering

(1) In this regulation, a reference to knowledge or suspicion does not include knowledge or suspicion resulting only from—

(a) electronic detection, by an approved intelligent transport system, of apparent tampering with that system; or

(b) the analysis of data produced by such a system.

(2) If TCA knows, or has reasonable grounds to suspect, that intelligent transport system equipment has been tampered with, TCA must report that fact to the Authority within 5 business days.

(3) If TCA knows, or has reasonable grounds to suspect, that approved intelligent transport system equipment has been tampered with, TCA must not disclose to any person other than the Authority—

(a) that the provider has that knowledge or suspicion; or

(b) any information from which the person to whom the disclosure is made could reasonably infer that TCA had that knowledge or suspicion.

(4) If TCA has made a report to the Authority of apparent tampering or suspicion of tampering, TCA must not disclose to any person other than the Authority—

(a) that the report has been made; or

(b) any information from which the person to whom the disclosure is made could reasonably infer that TCA had made such a report.

# Part 6—Duties, powers and obligations of IAP auditors

## 34—What IAP audit is

***IAP audit*** is the process of—

(a) reviewing IAP information held by an IAP service provider to determine its completeness and reliability; and

(b) reviewing the processes by which that information was collected; and

(c) examining how it is stored, used and disclosed; and

(d) examining IAP equipment installed in a vehicle or used by an IAP service provider.

## 35—IAP auditors' duties in regard to use and disclosure of information

(1) An IAP auditor must not use or disclose IAP information unless it first takes reasonable steps to ensure that, having regard to the purpose for which the information is to be used or disclosed, that the information is accurate, complete, up-to-date and not misleading.

(2) An IAP auditor must not use or disclose information for a purpose other than the purpose for which the information was collected.

(3) An IAP auditor must not use or disclose information relating to a particular participating operator other than to—

(a) the operator; or

(b) TCA; or

(c) the Authority,

unless the use or disclosure is authorised under these regulations or another law.

(4) An IAP auditor must not disclose information relating to non-compliance or tampering except to—

(a) the Authority; or

(b) TCA.

(5) If an IAP auditor uses or discloses IAP information (other than use or disclosure for law-enforcement purposes), the IAP auditor must make a record of the use or disclosure containing the following information:

(a) the name of the person who used or disclosed the IAP information;

(b) the date of the disclosure or use;

(c) in the case of a disclosure of IAP information, the person or body to whom or to which the information was disclosed;

(d) in the case of a use of IAP information, a brief description of how the information was used;

(e) what provision of these regulations or another law the disclosure or use was authorised by;

(f) if the authority for the disclosure or use also required a document (for example, a warrant, a certificate or a consent), a copy of the document.

(6) The IAP auditor must make the record within 5 business days after the relevant use or disclosure.

(7) The IAP auditor must make the record in a form that allows the record to be readily inspected.

(8) The IAP auditor must retain the record for 2 years.

(9) An IAP auditor commits an offence if it does not comply with a requirement of any of subregulations (1) to (8).

Maximum penalty:

(a) for a first offence—$10 000;

(b) for a second or subsequent offence—$20 000.

## 36—IAP auditors' powers to collect, store, use and disclose IAP information

(1) An IAP auditor may collect, store, use and disclose IAP information (including personal information) for—

(a) the performance of its functions; or

(b) to report, to TCA, non-compliance or tampering by a participating operator; or

(c) to report, to TCA, tampering by an IAP service provider, or a failure by an IAP service provider to comply with its obligations.

(2) An IAP auditor may use or disclose IAP information (including personal information)—

(a) with the consent of any person about whom the IAP information includes personal information; or

(b) as otherwise authorised by these regulations or any other law.

## 37—IAP auditors' obligations in regard to collecting IAP information

(1) An IAP auditor may collect IAP information that is reasonably necessary to enable the auditor to prepare an audit report on an IAP service provider.

(2) An IAP auditor must take reasonable steps to ensure that IAP information that it collects—

(a) is necessary for, or is directly related to, the purpose for which it is collected, or a directly related purpose; and

(b) is not excessive for that purpose; and

(c) is accurate, up-to-date and complete.

(3) An IAP auditor must take reasonable steps to ensure that the collection of IAP information does not intrude to an unreasonable extent on the personal privacy of any individual to whom the information relates.

## 38—IAP auditors' obligation to keep information secure

(1) An IAP auditor must take reasonable steps to protect IAP information collected by it against unauthorised access, unauthorised use, misuse, loss, modification or unauthorised disclosure.

(2) An IAP auditor must take reasonable steps to destroy personal information no longer needed for IAP purposes, or remove permanently from such information anything by which an individual can be identified.

## 39—IAP auditors' obligation to make individuals aware of personal information held

(1) If an individual so requests, an IAP auditor must take reasonable steps to inform him or her of—

(a) the kinds of information it holds about him or her; and

(b) the purpose for which the information is held; and

(c) the persons and authorities to which information so collected may be disclosed; and

(d) that the collection of the information is authorised by these regulations; and

(e) that he or she has the rights of reasonable access to, and of correction of, personal information so held, and how those rights can be exercised.

(2) An IAP auditor must, on request by an individual about whom the IAP auditor holds personal information, give him or her access to the information, and must do so without undue delay or cost.

## 40—IAP auditors' obligation to keep records of transactions

(1) An IAP auditor must keep and retain records, in accordance with this regulation, of its transactions with IAP service providers and TCA.

(2) The records must be organised in such a way as will enable them to be conveniently and properly audited.

## 41—IAP auditors' obligation to correct errors etc

(1) An IAP auditor must take reasonable steps to ensure that information that it collects is accurate, complete, up-to-date and not misleading.

(2) If so requested by a participating operator or an IAP service provider, an IAP auditor must make appropriate alterations to any information it holds to ensure that the information is accurate, complete, up-to-date and not misleading.

(3) If the IAP auditor considers that the information the subject of such a request is not inaccurate, incomplete, out-of-date or misleading, it may refuse to comply with the request, but must then—

(a) give the operator or service provider a statement in writing of its reasons for refusing; and

(b) if the operator or service provider so requests, attach to, or include with, the information a statement by the operator or service provider.

### 42—IAP auditors' obligation to report breaches by IAP service providers

If an IAP auditor knows of a breach by an IAP service provider of the provider's obligations under these regulations, or of anything that indicates that an IAP service provider may have breached such an obligation, the IAP auditor must, as soon as practicable, report that fact to TCA.

Maximum penalty:

(a) for a first offence—$10 000;

(b) for a second or subsequent offence—$20 000.

### 43—IAP auditors' obligation to report tampering

If an IAP auditor knows, or has reasonable grounds to suspect, that intelligent transport system equipment has been tampered with, the IAP auditor must, as soon as practicable, report that fact to—

(a) in the case of tampering or suspected tampering by a participating operator—the Authority; or

(b) in the case of tampering or suspected tampering by an IAP service provider—TCA.

Maximum penalty:

(a) for a first offence—$10 000;

(b) for a second or subsequent offence—$20 000.

## Part 7—Tampering with approved intelligent transport systems

### 44—Meaning of tampering

(1) A person ***tampers*** with an approved intelligent transport system if—

(a) he or she engages in conduct that has the result that—

(i) the system is altered; or

(ii) the system is installed or used in a way that is not in accordance with the conditions of its certification by TCA; or

(iii) any data instruction that the system uses internally is altered; and

(b) he or she does so with the intention of causing the system to—

(i) fail to collect IAP information, or fail to collect such information correctly; or

(ii) fail to store IAP information, or fail to store such information correctly; or

(iii) fail to report IAP information, or fail to report such information correctly.

(2) A person also ***tampers*** with an approved intelligent transport system if he or she—

(a) engages in conduct; and

(b) is negligent or reckless as to whether, as a result of the conduct, the system may—

(i) fail to collect IAP information, or fail to collect such information correctly; or

(ii) fail to store IAP information, or fail to store such information correctly; or

(iii) fail to report IAP information, or fail to report such information correctly.

(3) For subregulation (1) and (2)—

(a) a system ***fails*** if it does not perform as intended in terms of accuracy, timeliness, reliability, verifiability or any other performance parameter; and

(b) ***fail*** includes fail permanently, fail temporarily, fail on a particular occasion or occasions, and fail in particular circumstances.

### 45—Offence—tampering with approved intelligent transport system

A person must not tamper with an approved intelligent transport system.

Maximum penalty:

(a) if regulation 44(1)(b) applies—

(i) for a first offence—$20 000;

(ii) for a second offence—$50 000;

(b) if regulation 44(2)(b) applies—

(i) for a first offence—$10 000;

(ii) for a second offence—$20 000.

## Part 8—Evidence

### 46—References to particular time etc

In this Part—

***at a specified time*** includes on a specified date and during a specified period.

### 47—Certificates by the Authority

(1) A certificate signed on behalf of the Authority, and stating any of the following, is admissible in evidence and is prima facie evidence of what it states:

(a) that a specified IAP condition was in effect for a specified participating operator at a specified time;

(b) that a specified person is, or was at a specified time, a participating operator;

(c) that a specified IAP condition applied to a specified IAP vehicle at a specified time;

(d) that a specified vehicle is, or was at a specified time, an IAP vehicle;

(e) that a specified participating operator is, or was at a specified time, the operator of a specified IAP vehicle;

(f) that a specified non-compliance report, tampering report or IAP auditor's report was received at a specified time, or has not been received;

(g) that no report of a malfunction has been received, or had been received at a specified time, by the Authority in relation to an approved intelligent transport system fitted to a specified IAP vehicle;

(h) that a report of a specified malfunction was received at a specified time, or has not been received;

(i) that a specified form is an approved form for a specified purpose.

(2) A document purporting to be a certificate under subregulation (1) is presumed (unless evidence sufficient to raise doubt about the presumption is adduced) to be what it purports to be.

(3) The person who signed such a document is presumed (unless evidence sufficient to raise doubt about the presumption is adduced) to have been authorised by the Authority to do so.

## 48—Certificate as to intelligent access map

(1) TCA may certify in writing that a particular map is the intelligent access map as issued by TCA at a specified time.

(2) The map may be in the form of an electronic data file.

(3) A certificate under subregulation (1) is admissible in evidence and is conclusive evidence of what it states.

(4) The intelligent access map, as issued by TCA at a particular time, is presumed (unless evidence sufficient to raise doubt about the presumption is adduced) to be a correct representation of the national road network at the time of its issue.

(5) A document purporting to be a certificate under subregulation (1) is presumed (unless evidence sufficient to raise doubt about the presumption is adduced) to be what it purports to be.

(6) The person who signed such a document is presumed (unless evidence sufficient to raise doubt about the presumption is adduced) to have been authorised by TCA to do so.

## 49—Other certificates by TCA

(1) A certificate signed on behalf of TCA, and stating any of the following, is admissible in evidence and is prima facie evidence of what it states:

(a) that a particular intelligent transport system is, or was at a specified time, an approved intelligent transport system;

(b) that on a specified date a specified person was or was not an IAP service provider or an IAP auditor.

(2) A document purporting to be a certificate referred to in subregulation (1) is presumed (unless evidence sufficient to raise doubt about the presumption is adduced) to be what it purports to be.

(3) The person who signed such a document is presumed (unless evidence sufficient to raise doubt about the presumption is adduced) to have been authorised by TCA to do so.

## 50—Presumption of correct operation

The equipment and software that makes up an approved intelligent transport system is presumed (unless evidence sufficient to raise doubt about the presumption is adduced) to have operated correctly on any particular occasion.

## 51—Evidence as to vehicle's position

A statement of a vehicle's position on the surface of the earth at a particular time, in a non-compliance report or otherwise generated or produced by means of an approved intelligent transport system, is presumed (unless evidence sufficient to raise doubt about the presumption is adduced) to be a correct statement of the vehicle's position at the time.

## 52—IAP information generated etc by approved intelligent transport system

(1) IAP information generated by an approved intelligent transport system is presumed (unless evidence sufficient to raise doubt about the presumption is adduced) to have been correctly generated.

(2) IAP information recorded by an approved intelligent transport system is presumed (unless evidence sufficient to raise doubt about the presumption is adduced) to have been correctly recorded.

(3) IAP information stored by an approved intelligent transport system is presumed (unless evidence sufficient to raise doubt about the presumption is adduced) not to be changed by that storage.

(4) If it is established that some of such IAP information has been changed by being so stored, the presumption in subregulation (3) continues to apply to any other IAP information so stored.

## 53—Reports by approved intelligent transport system

(1) A non-compliance report, or a report under regulation 21, made by an approved intelligent transport system—

(a) is admissible in evidence; and

(b) is prima facie evidence of the facts stated in it; and

(c) is presumed (unless evidence sufficient to raise doubt about the presumption is adduced) to be a correct report of information generated and recorded by the system.

(2) A report made by an approved intelligent transport system setting out IAP information—

(a) is admissible in evidence; and

(b) is prima facie evidence of the facts stated in it; and

(c) is presumed (unless evidence sufficient to raise doubt about the presumption is adduced) to be a correct report of information generated and recorded by the system.

(3) If it is established that a part of such a report is not a correct report of the relevant part of the IAP information as so recorded, the presumption in subregulation (1)(c) or (2)(c) continues to apply to the remainder of the report.

(4) A document that purports to be a report made by an approved intelligent transport system is presumed (unless evidence sufficient to raise doubt about the presumption is adduced) to be such a report.

## 54—Results of mathematical procedures

(1) A certificate signed on behalf of the Authority—

(a) stating that a specified mathematical (including statistical) procedure was carried out in relation to IAP information specified or referred to in the certificate; and

(b) setting out the results of doing so,

is admissible in evidence and is prima facie evidence of the facts stated in it.

(2) The specified procedure is presumed (unless evidence sufficient to raise doubt about the presumption is adduced)—

(a) to be valid and reliable for the purpose for which it was used; and

(b) to have been carried out correctly.

(3) A document that purports to be a certificate mentioned in subregulation (1) is presumed (unless evidence sufficient to raise doubt about the presumption is adduced) to be what it purports to be.

(4) The person who signed such a document is presumed (unless evidence sufficient to raise doubt about the presumption is adduced) to have been authorised by the Authority to do so.

## Made by the Governor

with the advice and consent of the Executive Council
on 5 November 2009

No 265 of 2009

MTR08/045