LBS

TERMS AND CONDITIONS

1. Introduction

1.1 In the circumstances the INTEGRAT Service agreement concluded between the parties is hereby supplemented with the following Terms and Conditions, which shall apply in the event of the CLIENT being permitted use LBS.

2. Definitions

There are typically three types of LBS requests called active, passive and tracking requests. Similarly, CLIENTs will typically deploy three types of LBS services.

2.1 Active Location Based Services

2.1.1 "Active LBS" means those LBS services that are initiated by a Service User utilising a mobile phone, and the response is sent by the WASP, using the location of the mobile phone. In most cases the Requestor/A-party will be the Target/B-party. These services are also sometimes known as "pull" services.
2.1.2 Active LBS involves the Service User requesting an LBS service that relies on the user's own geographical location for completion of the LBS service. Examples include finding places of interest, local news or weather forecasts and the like. There is an implicit consent to location-based information being analysed and possibly passed on to a CLIENT or other third party (such as a third party data base provider or content provider) if necessary to provide the LBS service.

2.2 Passive Location Based Services

2.2.1 "Passive LBS" means those LBS services where a Service User (the Target/B-party), once s/he has enabled an LBS service, consents to being located by a CLIENT to provide an LBS service to which the Target/B-party has subscribed.

2.2.2 Passive LBS is initiated by the CLIENT rather than the Service User, but based on the Target/B-party's request for an LBS service, such as traffic or weather information to be provided on a regular basis, as opposed to once off requests. In order for the CLIENT to provide the LBS service (such as local traffic update at 07h00 each morning before the Service User leaves for work) the CLIENT must confirm the Target/B-party's location.

2.2.3 Deploying passive LBS services requires the B-Party to give consent by subscribing to a specific LBS service. In most cases the Requestor/A-party will be the Target/B-party.

2.3 Tracking Location Based Services

2.3.1 Access to LBS for the Tracking Location Based Services is to be used when the Service User i.e. the Target/B-party, has firstly enabled a service and provided consent to being located by another party or the requestor. This indicates an existence of a relationship between the A-Party and the B-Party that is governed firstly, by the need for the service by the B-party which the B-party exercises by enabling the service and secondly providing the express consent to confirm such.

2.3.2 Tracking LBS services involve locating a Target/B-party as requested by a Requestor/A-party based on the location of the SIM card associated with the Target/B-party, either on its own or as part of a combination of technologies.

2.3.3 Emergency tracking by means of the Vodacom LBS service will therefore only be allowed if the B-party, has firstly enabled such a service and has provided consent to be located by the A-Party, which then eliminates the sense of emergency because the relationship and consent would have been pre-existing and the A-Party can locate the B-party whenever required including in cases of emergency.

2.3.3 All references in this document to these Terms and Conditions shall be deemed to include a reference to the audit criteria recorded in the LBS Audit Criteria document.

3. INTEGRAT Service Agreement and network prerequisites

3.1 The CLIENT shall comply with these Terms and Conditions and shall continue to be bound by the INTEGRAT Service agreement. In the event of any contradiction between these Terms and Conditions and the INTEGRAT Service Agreement, then these Terms and Conditions shall take precedence for LBS Services. The phrases used in these Terms and Conditions shall, unless the context clearly indicates otherwise, have the same meaning as assigned to them in the INTEGRAT Service Agreement. It is recorded that the definition of “the Bearer” in the INTEGRAT Service Agreement shall be deemed to include location based type services.

3.2 In the event of the CLIENT using LBS for any fraudulent or mala fide purpose or for any other purpose for which it was not intended, then INTEGRAT shall be entitled, immediately and without notice, to suspend the CLIENTS’s right to use LBS.

3.3 Prior to approving the application by the CLIENT to deploy LBS services (and at all times after approval may have been obtained), INTEGRAT shall at its sole and absolute discretion (and by whatever means as INTEGRAT may deem appropriate including but not limited to random tests) be entitled but not obliged to determine whether the CLIENTS’ systems are sufficiently secure and whether the processes by which the CLIENT utilize LBS, are appropriate and sufficiently secure.

3.4 Prior to being permitted to deploy LBS services the CLIENT shall be required to submit a certificate from an independent and accredited IT Audit Company confirming that it complies with these Terms and Conditions.

3.5 The cost of the audit referred to in clause 3.4 above shall be for the CLIENT's account, and INTEGRAT shall be entitled to require the CLIENT to have similar audits carried out on its systems at such intervals as INTEGRAT may determine. The production of an audit certificate as envisaged in clause 3.4 above shall not necessarily mean that the CLIENT's application to deploy LBS services shall be approved.

3.6 In the event that INTEGRAT determines (as it in its sole and absolute discretion may do) that the CLIENT cannot or has not complied, or can no longer comply with these Terms and Conditions, then INTEGRAT may immediately and without notice reject the CLIENTS's application to deploy LBS services or once deployed, immediately and without notice suspend the CLIENTS's right to use LBS services.

3.7 The CLIENT shall be required to make separate applications for each LBS service that it desires to launch, each of which shall be considered by INTEGRAT separately.

4. Regulatory Criteria

4.1 The privacy of the customer must be protected at all times, and under no circumstances may the customer's location or details be provided to any third party, entity or application without that customer's specific and express consent to the NETWORK for the specific and identified third party, entity or application to receive such information.

4.2 Authorisation / consent

4.2.1 The customer's location may not be used or divulged to 3rd parties, unless the customer gives his prior specific authorisation/consent to NETWORK per each individual third party attempting to locate them – either in writing (subscription services) or electronically (via website, SMS, USSD etc.) subject to the condition that the customer can be successfully authenticated.

4.2.2 Consent always needs to be specific in that the customer has to know exactly what s/he is consenting to. Consent must be on a service-by-service basis.

4.2.3 No anonymous Requestors/A-parties will be allowed, as the Target/B-party should always have authorised the capability of being located by the specific A-party either during subscription or on a once-off basis.

4.2.4 In the case of Active LBS and Passive LBS services, discrete authorizations can be done each time an LBS service is requested and there is no issue with an on-going consent, as in the case of

tracking LBS services. In the case of certain proposed emergency LBS services (which display a combination of features of Active LBS and Tracking LBS services) discrete authorizations can be obtained using an interactive voice system so as to fall within the ECT Act.

4.2.5 In the circumstance where there are two separate customers for one SIM card, i.e. the owner of the contract/SIM card and the user of the SIM card – e.g. where an employer signs a contract for a SIM card, which is in turn used by an employee, then the consent of the customer in *de facto* control of the handset and thus the recipient of the telecommunications service must be sent to the NETWORK.

4.2.6 In order for consent to be extended an "opt-out" reminder must be sent on a 30 day basis to the Target/B-party.

4.2.7 The Target/B-party may withdraw the authorisation or opt-out at any time and must be able to suspend the authorisation for either a fixed or indefinite period should the Target/B-party instruct NETWORK to do so.

4.3 Other conditions

4.3.1 The Target/B-party must be able to opt-out of being located at any time that s/he wishes to do so.

4.3.2 It should further be possible for a Target/B-party to specify the period of the day or day(s) of the week, month(s) or year during which a specific Requestor/A-party will be authorised to locate him/her and should only be located by the relevant Requestor/A-party during this period.

4.4 Registration

4.4.1 The CLIENT, the A-party (party requesting the location information) and the B-party (customer being located) must register for the service with INTEGRAT as per clause 3.5.

4.4.2 Especially with regard to Tracking LBS services with regard to a person, the Target/B-party must be invited to register with the CLIENT and to add Requestors/A-parties who may use the LBS service to locate the Target/B-party. The Target/B-party must then be able to choose the period of "each occasion" before the authorisation will expire and must renew at. The target/B-party can be given the option of a variety of different time periods by which to renew his consent, provided that the maximum period shall be no longer than 30 days.

4.5 Record storing
The CLIENT must ensure that all communication with the customer and INTEGRAT'S platform are properly recorded and stored for as long as the CLIENT is legally required to do this. If there is no legal requirement, the CLIENT should store the collected information for a minimum period of 5 years.

4.6 WASP: Authentication

The CLIENT will be authenticated by INTEGRAT on each request for location information in accordance with the process set out above.

4.7 Warranties and Disclaimers

4.7.1 INTEGRAT does not give any warranties with regard to the accuracy of the LBS services and the CLIENT must ensure that no such warranties are given to the Service Users.

4.7.2 Disclaimers must be in place in the contracts between the CLIENT, and the A-party and B- party. Some form of disclaimer must also appear within all advertising relating to LBS. The following disclaimer is suggested:
a. Neither [name of CLIENT], INTEGRAT (Pty) Ltd or Network any of their affiliate companies, agents, distributors, members, officers, agents, directors, employees, servants or the like shall assume responsibility or be liable for any losses, costs, damages, expenses, claims, (whether direct, indirect, special or consequential), or injuries or death, incurred or sustained by any person, whether arising directly or indirectly from the use or misuse by any person of, or the provision by [name of CLIENT], INTEGRAT (Pty) Ltd or Network or, failure by [name of CLIENT] or INTEGRAT (Pty) Ltd or GSM Network to provide, the location based service.
b. You acknowledge that the accuracy of the location service is determined by the density of the cell centroid which will vary from one cell to another. You acknowledge that the NETWORK cannot guarantee and shall not be responsible for the accuracy of the service. You acknowledge and accept that quality and coverage of the service shall be limited to that provided by the NETWORK and the services may, from time to time, be adversely affected by physical features such as buildings and underpasses, as well as atmospheric conditions and other causes of interference.

4.8 Customer Education

Customers must be advised that should they use an LBS service their location information will be used by and disclosed to the CLIENT, but will only be used for the specific purposes for which they have provided consent.

4.9 Third parties

The CLIENT shall ensure that in any agreement it enters into with any of its sub-contractors, agents, partners, suppliers or the like regarding any matter relating to the LBS Services, or should any of the CLIENT's rights as provided for herein be exercised through such persons, then it shall bind such persons to the same obligations to which it is bound in terms of these terms and conditions, as may be applicable in the circumstances, and shall ensure that their exercise of such rights do not contravene these terms and conditions. Furthermore the CLIENT shall be responsible for the acts or omissions of such persons that contravene these terms and conditions.

4.10 Security and Risk

Under no circumstances can the LBS platform be used for location based services related to Law Enforcement or Police investigations. No Company or individual cell phone can be tracked unlawfully. *The Regulation of Interception of Communications and provision of Communication-related Information Act, 2002 ("the Interception and Monitoring Act')* supersedes any provision made for any legal disclosure of location based information, of which *section 7 and 8 make provision for the disclosure in certain circumstances for LBS:*

- *Section 7: Interception of Communication to prevent serious bodily harm.*
- *Section 8: Interception of Communication for purposes of determining location in case of emergency.*

Law Enforcement agencies rely on the provisions of the *Interception and Monitoring Act* to obtain any information from the NETWORK. The Police Services have established units within their structures which are responsible for interfacing with the NETWORKS and the NETWORKS explicitly only deals with this unit i.e. OCIM OFFICE – i.e. OFFICE COMMUNICATION, INTERCEPTION & MONITORING. Any Police officer that requires any information approaches this office (OCIM) and the OCIM OFFICE authenticates the request and is responsible for making contact with the NETWORK in accordance with all applicable rules and procedures.

Private investigators have no power whatsoever to use the NETWORK's LBS platform to provide services to third parties for tracking purposes. Tracing of handsets and tracing MSISDN numbers without any consent is a clear breach of the Interception and Monitoring Act, and CLIENTS having access to LBS and using of it for unlawful purposes will be suspended immediately.

Any person or any employee of the CLIENT that intentionally discloses information in contravention of the Interception and Monitoring Act, or unlawfully intercepts communication, will face a fine of up to R2mil or imprisonment for a period not exceeding 10 years.

4.11 Regulation Summary

- There are predominantly two pieces of legislation that the majority of requests make use of to disclose or intercept information.
- Criminal Procedures Act 51 of 1977 and the Regulation on Interception of Communication and Provision of Communication –Related Information Act 70 of 2002.
- The Subpoena's or Directives request multiple kinds of information, from Call Data, RICA Registration, Opening Documents, Interceptions and Location Based services. All of the above information is archived for 3 years in compliance to the Act.
- The NETWORK has developed an automated process, which the SAPS TSU uses to request information via our system that is securely accessible over the Internet Protocol. Once the information has been extracted, it is submitted via the same system back to the TSU.
- Comply to different pieces of legislation, including the provisions of section 7 and 8 of Act 70 of 2002, which deals with Location based information, the circumstances under which the content can be provide to prevent serious bodily harm or determine location in a case of an emergency.

4.11.1 Section 7 and 8 of Act 70 of 2002

SECTION 7: Interception of communication to prevent serious bodily harm - Act 70 of 2002

1) Any law enforcement officer may, if-

(a) he or she is satisfied that there are reasonable grounds to believe that a party to the communication has-

(i) Caused or may cause the infliction of serious bodily harm to another person;

(ii) threatens or has threatened to cause the infliction of serious bodily harm to another person; or

(iii) threaten or has threatened, to take his or her own life or to perform an act which would or may endanger his or her own life or would or may cause the infliction of serious bodily harm to himself or herself;

(b) he or she is of the opinion that because of the urgency of the need to intercept the communication, it is not reasonably practicable to make an application in terms of section 16(1) or 23(1) for the issuing of an interception direction or an oral interception direction; and

(c) the sole purpose of the interception is to prevent such bodily harm, intercept any communication or may orally request a telecommunication service provider to route duplicate signals of indirect communications specified in that request to the interception centre designated therein.

(2) A telecommunication service provider must upon receipt of a request made to him or her in terms of subsection (1), route the duplicate signals of the indirect communications concerned to the designated interception centre.

(3) The law enforcement officer who made a request under subsection (1) must as soon as practicable after making that request furnish the telecommunication service provider concerned with a written confirmation of the request which sets out the information given by that law enforcement officer to that telecommunication service provider in connection with the request.

(4) The law enforcement officer who intercepts a communication under subsection (1) or (2) must as soon as practicable after the interception of the communication concerned, submit to a designated judge

(a) a copy of the written confirmation referred to in subsection (3);

(b) an affidavit setting forth the results and information obtained from that interception: and

(c) any recording of the communication that has been obtained by means of that interception any full or partial transcript of the recording and any notes made by that law enforcement officer of the communication if nothing in the communication suggests that bodily harm attempted bodily harm or threatened bodily harm has been caused or is likely to be caused.

(5) A telecommunication service provider who in terms Of subsection (2) has routed duplicate signals of indirect communications to the designated interception centre must as soon as practicable thereafter submit an affidavit to a designated judge setting forth the steps taken by that telecommunication service provider in giving effect to the request concerned and the results obtained from such steps.

(6) A designated judge must keep all written confirmations and affidavits and any recordings, transcripts or notes submitted to him or her in terms of subsections (4) and (5) or cause it to be kept. for a period of at least five years.

SECTION 8: Interception of communication for purposes of determining location in case of emergency - Act 70 of 2002

1) In circumstances where –

a) a person is a party to a communication;

b) that person, as a result of information received from another party to the communication (in this section referred to as the "sender"), has reasonable grounds to believe that an emergency exists by reason of the fact that the life of another person, whether or not the sender, is being endangered or that he or she is dying or is being or has been seriously injured or that his or her life is likely to be endangered or that he or she is likely to die or to be seriously injured; and

c) the location of the sender is unknown to that person, the person referred to in paragraph (a) may, if he or she is –

i) a law enforcement officer, and if he or she is of the opinion that determining the location of the sender is likely to be of assistance in dealing with the emergency, orally request, or cause another law enforcement officer to orally request, the telecommunication service provider concerned to –

(aa) intercept any communication to or from the sender for purposes of determining his or her location; or

(bb) determine the location of the sender in any other manner which the telecommunication service provider deems appropriate; or

ii) not a law enforcement officer, inform, or cause another person to inform, any law enforcement officer of the matters referred to in paragraphs (a), (b) and (c).

2) A law enforcement officer who has been informed as contemplated in subsection (1)(ii), may, if he or she is of the opinion that determining the location of the sender is likely to be of assistance in dealing with the emergency, orally request, or cause another law enforcement officer to orally request, the telecommunication service provider concerned to act as contemplated in subsection (1)(i)(aa) or (bb).

3) A telecommunication service provider must, upon receipt of a request made to him or her in terms of subsection (1)(i) or (2) –

a) intercept any communication to or from the sender for purposes of determining his or her location; or

b) determine the location of the sender in any other manner which the telecommunication service provider deems appropriate, and if the location of the sender has been so determined, the telecommunication service provider concerned must, as soon as practicable after determining that location, provide the law enforcement officer who made the request with the location of the sender and any other information obtained from that interception which, in the opinion of the telecommunication service provider concerned, is likely to be of assistance in dealing with the emergency.

The law enforcement officer who made a request under subsection (1)(i) or (2) must –

a) as soon as practicable after making that request, furnish the telecommunication service provider concerned with a written confirmation of the request which sets out the information given by that law enforcement officer to that telecommunication service provider in connection with the request;

b) as soon as practicable after making that request, furnish a designated judge with a copy of such written confirmation; and

c) if the location of the sender and any other information has been provided to him or her in terms of subsection (3), as soon as possible after receipt thereof, submit to a designated judge an affidavit setting forth the results and information obtained from that interception.

5) A telecommunication service provider who has taken any of the steps contemplated in subsection (3), must, as soon as practicable thereafter, submit to a designated judge –

a) an affidavit setting forth the steps taken by that telecommunication service provider in giving effect to the request concerned and the results and information obtained from such steps; and

b) if such steps included the interception of an indirect communication, any recording of that indirect communication that has been obtained by means of that interception, any full or partial transcript of the recording and any notes made by that telecommunication service provider of that indirect communication.

6) A designated judge must keep all written confirmations and affidavits and any recordings, transcripts or notes submitted to him or her in terms of subsections (4)(b) and (c) and (5), or cause it to be kept, for a period of at least five years.

4.11.2 Act 70 of 2002 Section 51 – Offences and Penalties

1)

a) Any person who –

i) contravenes or fails to comply with section 6(2), 7(4), 8(4), 29(8), 42(1) or 45(1);

ii) in any application made in terms of this Act, furnishes information or makes a statement, knowing such information or statement to be false, incorrect or misleading or not believing it to be correct;

iii) acts contrary to the authority of any direction issued under this Act or proceeds to act under any such direction knowing that it has expired;

iv) acts contrary to the authority of an entry warrant issued under this Act or, without being authorised thereto under an entry warrant, enters any premises for purposes of intercepting a postal article or communication, or installing and maintaining an interception device, on that premises;

v) forges or, with the intent to deceive, alters or tampers with any direction or entry warrant issued under this Act;

vi) furnishes particulars or information in any affidavit or report referred to in this Act, knowing such particulars or information to be false, incorrect or misleading or not believing it to be correct; or

vii) obstructs, hinders or interferes with an authorised person who executes any direction or entry warrant issued under this Act or assists with the execution thereof, in the exercising of his or her powers under that direction or entry warrant, is guilty of an offence.

b) Any person who is convicted of an offence referred to in—

i) paragraph (a) or in section 49(1) or 54, is liable to a fine not exceeding R2 000 000 or to imprisonment for a period not exceeding 10 years; or

ii) section 52, 53(1) or 55(1), is liable to a fine or to imprisonment for a period not exceeding two years.

2)

a) Any postal service provider or employee of a postal service provider who –

i) contravenes or fails to comply with section 28(1)(X);

ii) contravenes or fails to comply with section 42(2); or

iii) performs an act contemplated in subsection (l)(FAQ)(iii), (v) or (vii), is guilty of an offence.

b) Any postal service provider or employee of a postal service provider who is convicted of an offence referred to in paragraph (a) is liable, in the case of—

i) a postal service provider who is

(aa) natural person, to a fine not exceeding R2 000 000 or to imprisonment for a period not exceeding 10 years; or

(bb) juristic person, to a fine not exceeding R5 000 000; or

ii) an employee, to a fine not exceeding R2 000 000 or to imprisonment for a period not exceeding 10 years

3)

a) Any telecommunication service provider or employee of a telecommunication service provider who—

i) contravenes or fails to comply with section 7(2), 8(3), 29(l)(b) or (2), 30(1) or 39(4);

ii) contravenes or fails to comply with section 30(4);

iii) contravenes or fails to comply with section 7(5), 8(5), 39(1) or (2) or 42(2); or

iv) performs an act contemplated in subsection (l)(a)(iii), (v) or (vii), is guilty of an offence.

b) Any telecommunication service provider or employee of a telecommunication service provider who is convicted of an offence referred to in paragraph (a) or in section 50(1), is liable, in the case of—

i) a telecommunication service provider who is FAQ—

(aa) natural person, to a fine not exceeding R2 000 000 or to imprisonment for a period not exceeding 10 years; or

(bb) juristic person, to a fine not exceeding R5 000 000; or

ii) an employee, to a fine not exceeding R2 000 000 or to imprisonment for a period not exceeding 10 years.

3A) Any electronic communication service provider who fails to comply with—

a) the directives issued in terms of section 30(2)(a);

b) section 40(1), (2), (3), (4) or any determination made thereunder, (6), (7), (9) or (10); or 40

c) section 62(6)(a), (b), (c) or (d), is guilty of an offence and liable on conviction to a fine not exceeding R100 000 for each day on which such failure to comply continues.

3B) Any customer or person who fails to comply with section 40(5) is guilty of an offence and liable on conviction to a fine or to imprisonment for a period not exceeding 12 months.

3C) An employee or agent of an electronic communication service provider who fails to comply with section 40(8), is guilty of an offence and liable on conviction to a fine or to imprisonment for a period not exceeding 12 months.

3D) Any—

a) juristic person contemplated in section 62C(1); or

b) person contemplated in section 62C(2), who fails to comply with section 62C, is guilty of an offence and liable on conviction to a fine not exceeding R2 000 000 or to imprisonment for a period not exceeding 10 years.

4)

a) Any decryption key holder or any employee of a decryption key holder who—

i) contravenes or fails to comply with section 29(1);

ii) contravenes or fails to comply with section 29(2), (3)(b), (5) or (7) or 42(2); or

iii) performs an act contemplated in subsection (l)(a)(iii), (v) or (vii), is guilty of an offence.

b) Any decryption key holder or employee of a decryption key holder who is convicted of an offence referred to in paragraph (a) is liable, in the case of—

i) a decryption key holder who is FAQ—

(aa) natural person, to a fine not exceeding R2 000 000 or to imprisonment for a period not exceeding 10 years; or

(bb) juristic person, to a fine not exceeding R5 000 000; or

ii) an employee, to a fine not exceeding R2 000 000 or to imprisonment for a period not exceeding 10 years.

5) A conviction of an offence referred to in—

a) subsection (2)(FAQ)(i) does not relieve any postal service provider or any employee of such a postal service provider of the obligation to comply with section 28(1)(FAQ);

b) subsection (3)(FAQ)(i) or (ii) does not relieve any telecommunication service provider or any employee of such a telecommunication service provider of the obligation to comply with section 2&(l)(b) or (2), 30(1) or (4) or 39(4);

bA) subsection (3A) does not relieve any electronic communication service provider of the obligation to comply with—

i) the directives issued in terms of section 30(2)(a);

ii) section 40(1), (2), (3), (4) or any determination made thereunder (6), (7), (9) or (10); or

iii) section 62(6)(a), (b), (c) or (d); or

c) subsection (4)(FAQ)(i) does not relieve any decryption key holder or any employee of such a decryption key holder of the obligation to comply with section 29(1).

6) Notwithstanding anything to the contrary in any other law contained, a magistrate's court may impose any penalty provided for in this Act.

7) No person who—

a) in good faith assists an authorised person with the execution of a direction; and

b) believes on reasonable grounds that such authorised person is acting in accordance with such a direction, is liable to prosecution for a contravention of this Act.

4.12 General

These Terms and Conditions are deemed to form part of the INTEGRAT Service Agreement. Upon the signing of these Terms and Conditions and making use of the LBS services provided by **INTEGRAT** the **CLIENT** declares and acknowledges that it has taken note of and has informed of itself of all information referred to herein.

DATED at _____ this ____ day of _____ 20___

AS WITNESSES:

1. _____

2. _____ _____

NAME:

INTEGRAT (Duly Authorized)

TITLE:

DATED at _____ this ____ day of _____ 20___

AS WITNESSES:

1. _____

2. _____ _____

NAME:

The CLIENT (Duly Authorized)

TITLE: