GRENADA

TELECOMMUNICATIONS (Confidentiality in Network & Services) REGULATIONS 20[- -]

ARRANGEMENT OF REGULATIONS

ARRANGMENT OF REGULATIONS

GRENADA

STATUTORY RULES AND ORDERS No. …….. OF 20[- -]

In exercise of the power conferred by section 73 of the Telecommunications Act 2000 (Act No. 31 of 2000) the Minister makes the following Regulations –

PART I
PRELIMINARY

Citation

1. These Regulations may be cited as the –
   TELECOMMUNICATIONS (CONFIDENTIALITY IN NETWORKS AND SERVICES) REGULATIONS.

2. **Interpretation**
   In these Regulations -
   "**Act**" means the Telecommunications Act 2000;
   "**authorized request**" means a request received from the recipient of a transmission;
   "Minister" means the Minister responsible for Telecommunications;
   "**subscriber personal information**" means information of a personal nature relating to a telecommunications subscriber that discloses the address, marital status, financial status, occupation or other identifying information that is unrelated or incidental to the provision of telecommunications services;
   "**subscriber proprietary network information**" means information that relates to the quantity, technical configuration, type, destination, and amount of use of a telecommunications service subscribed to by any subscriber of a telecommunications provider, and that is made available to the telecommunications provider by the subscriber solely by virtue of the customer-provider relationship.

PART II
INTERCEPTION MONITORING AND STOPPAGE

3. Activation of intercepted communication
A telecommunications provider must ensure that any interception of communications within its network is capable of being activated only when authorised by the receiver of a transmission, or in accordance with a court order.

4. Strict measures of control
A telecommunications provider shall -

(a) appoint a senior employee or officer with the responsibility for ensuring that the interception of communications can be activated only when authorised by the receiver or in accordance with a court order; and

(b) authorise designated employees or officers to engage where necessary in lawful interception activities.

5. Court order

A telecommunications provider must not implement any interception of transmissions over a public telecommunications network or telecommunications apparatus unless the telecommunications provider receives a court order authorising law enforcement officials to intercept transmissions over the public telecommunications network or apparatus.

6. Officials to act within strict guidelines

A telecommunications provider shall ensure that any employee or officer that it appoints pursuant to regulation 5 only effects interceptions that are authorised and except to a person who has made an authorised request, or when authorised by a court order to a law enforcement official.

7. Employee to execute agreement

(1) An employee of a telecommunications provider who is designated and authorised to receive and implement interception orders, or certifications, must execute a non-disclosure agreement which must be kept as part of that employee's permanent records.

(2) The terms of the agreement referred to in paragraph (1) survives any reassignment of the employee to other duties, or the termination or departure of the employee from the employment of the telecommunications provider.

8. Report of improper activities

(1) A telecommunications provider must report to law enforcement officials without delay any act –

(a) of unlawful electronic surveillance that has occurred on its premises; and

(b) which compromises the duty to report once the provider becomes aware.

(2) A telecommunications provider must report to law enforcement officials without delay any transmission which is accepted and which appears likely to threaten the national security or is contrary to public order.

9. Employee's suspension of duties pending investigation

(1) If there are reasonable grounds to suspect that an employee of a telecommunications provider is about to engage or may have engaged in illegal surveillance activity, that employee must be reassigned to other duties or suspended pending the outcome of an investigation.

(2) An employee who has been reassigned or suspended must not be allowed to have access to any equipment whereby proper investigations may be compromised.

10. Accurate records of interception

(1) A telecommunications provider must maintain accurate, complete and secure records of any interception of communications.

(2) Records of any interception of communication must include the –

(a) court order or ministerial directive;

(b) identity of the law enforcement officer who presented the court order;

(c) name and signature of the telecommunications provider's employee responsible for overseeing the interception of the communications;

(d) start date and time of the interception;

(e) telephone and circuit identification number or numbers involved; and

(f) telegraphic, facsimile, telephonic or any other such type of communication.

(3) The records of interception must be compiled either contemporaneously, or within a reasonable period of time following the initiation of the interception of the communications and such period must not exceed 90 days.

(4) A telecommunications provider must maintain a record of all intercepted communications for a period of 6 years.

11. Reporting obligations to Commission

(1) A telecommunications provider must report to the Commission on a quarterly basis any -

(a) compromises or suspected compromises of interceptions; and

(b) violation of its security policies and procedures.

(2) A telecommunications provider must report to the Commission without delay any violation or compromise relating to subscriber's -

(a) personal information; or

(b) proprietary network information.

12. No acceptance of dangerous transmission

A telecommunications provider must not accept any form of transmission which appears likely to threaten the national security or which is contrary to public order in Grenada.

PART III
NON-INTERCEPTION OF TRANSMISSIONS BY MEMBERS OF THE PUBLIC

13. No interception by members of public

Any member of the public, including a radio amateur using radio equipment or modified commercial equipment, must not intercept or interrupt any message transmitted over a public telecommunications network or telecommunications apparatus.

14. Reporting obligation on illegal activity

Where there are reasonable grounds to suspect that a member of the public is about to or is in the process of engaging in illegal surveillance activity, the telecommunications provider or any concerned party must report the activity to law enforcement officials without delay.

15. Reporting obligation of actual illegal activity

A telecommunications provider must report to the Commission and law enforcement officials without delay any act of unlawful electronic surveillance by an unauthorised member of the public that has occurred on its premises.

PART IV
CONFIDENTIALITY IN RESPECT OF SUBSCRIBERS

16. Strict control measures

A telecommunications provider must establish policies and procedures to facilitate the strictest supervision and control of its employees or officers who have or might have access to subscriber personal information or subscriber proprietary network information.

17. Employee to execute agreement

(1) An employee of a telecommunications provider who has access to subscriber personal information or subscriber proprietary network information must execute a non-disclosure agreement which must be kept as part of that employee's permanent records.

(2) The terms of the agreement referred to in paragraph (1) survives any reassignment of the employee to other duties or the termination or departure of the employee from the employment of the telecommunications provider.

18. Confidentiality of subscriber

The subscriber's personal information or subscriber's proprietary network information is confidential information, and must not be disclosed by an employee or officer of a telecommunications provider without the consent of the subscriber or pursuant to a court order.

19. Permission to be first obtained

A telecommunications provider or publisher of subscriber lists and directories must first obtain the consent of a subscriber before listing the subscriber's personal information in a telephone directory.

20. Grounds for disclosure of proprietary network information

A telecommunications provider may use or disclose subscriber proprietary network information only if it is necessary to -

(a) protect users of those services and other telecommunications providers from fraudulent, abusive or unlawful use of, or subscription to such services; or

(b) provide the telecommunications services to which the proprietary customer has subscribed.

Made this …….day of ……..…., 20[- -].

GREGORY BOWEN

Minister responsible for Telecommunications