### SAINT VINCENT AND THE GRENADINES

## TELECOMMUNICATIONS (CONFIDENTIALITY IN NETWORKS AND SERVICES) REGULATIONS, 2002

### ARRANGEMENT OF REGULATIONS

### REGULATION

### PART I – PREMILINARY

- 1. Citation and commencement
- 2. Interpretation

### PART 11 – INTERCEPTION MONITORING STOPPAGE

- 3. Activation of intercepted communication
- 4. Strict measures of control
- 5. Court order
- 6. Officials to act within strict guidelines
- 7. Employee to execute agreement
- 8. Report of improper activities
- 9. Employee's suspension of duties ending investigation
- 10. Accurate records of interception
- 11. Reporting obligations to Commission
- 12. No acceptance of dangerous transmission

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

- 13. No interception by members of public
- 14. Reporting obligation on illegal activity
- 15. Reporting obligation on actual illegal activity

### PART IV - CONFIDENTIALITY IN RESPECT OF SUBSCRIBER

- 16. Strict control measures
- 17. Employee to execute agreement
- 18. Confidentiality of subscriber
- 19. Permission to be first obtained
- 20. Grounds for disclosure of proprietary network information

### SAINT VINCENT AND THE GRENADINES

### STATUTORY RULES AND ORDERS

2002 NO. 10

2002 NO. 10	

(GAZETTED 31st January 2002)

<del>-----</del>

**IN EXERCISE** of the powers conferred by section 72 of the Telecommunications Act, 2001 the Minister makes the following Regulations:

## TELECOMMUNICATIONS (CONFIDENTIALITY IN NETWORKS AND SERVICES) REGULATIONS, 2002

### PART I PRELIMINARY

## Citation and commencement

- 1. (1) These Regulations may be cited as the Telecommunications (Confidentiality in Networks and Services) Regulations, 2002.
- (2) These Regulations shall come into force on the 1<sup>st</sup> day of February, 2002.

### Interpretation

### 2. In these Regulations

No. 1 of 2001

- "Act" means the Telecommunications Act, 2001;
- "authorised request" means a request received from the recipient of a transmission;
- "subscriber personal information" information of a personal nature relating to telecommunications subscriber address, marital status, discloses the financial status. occupation or other identifying information that is unrelated or incidental provision to the 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 STOPPAGE

## Activation of intercepted communication

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

## Strict measures of control

- 4. 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.

#### Court order

5. A telecommunications provider shall 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.

## Officials to act within strict guidelines

6. A telecommunications provider shall ensure that an employee or officer that it appoints pursuant to regulation 4 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.

## Employee to execute agreement

- 7. (1) An employee of a telecommunications provider who is designated and authorised to receive and implement an interception order or certification shall execute a non-disclosure agreement that shall be kept as part of that employee's permanent records.
- (2) Pursuant to sub-regulation (1) the terms of the agreement shall survive any reassignment of the employee to other duties, or the termination or departure of the employee from the employment of the telecommunications provider.

### Report of improper activities

- 8. (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) that compromises the duty to report once the provider becomes aware.
- (2) A telecommunications provider must report to law enforcement officials without delay any transmission that is accepted and appears likely to threaten the national security or is contrary to public order.

# Employee's suspension of duties ending investigation

- 9. (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 shall be reassigned to other duties or suspended pending the outcome of an investigation.
- (2) An employee who has been reassigned or suspended shall not be allowed to have access to any equipment that may compromise proper investigations.

## Accurate records of interception

- 10. (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;

- (b) identity of the law enforcement officer who presented the court order;
- (c) name and signature of the telecommunications provider's employee who is responsible for overseeing the interception of the communications;
- (d) commencement 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 the period shall not exceed ninety days.
- (4) A telecommunications provider must maintain a record of all intercepted communications for a period of six years.

## Reporting obligations to Commission

- 11. (1) A telecommunications provider shall 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 shall be obligated to report to the Commission without delay any violation or compromise relating to the subscriber's
  - (a) personal information; or
  - (b) proprietary network information.

No acceptance of dangerous transmission

12. A telecommunications provider must not accept any form of transmission that appears likely to threaten the national security or is contrary to public order in Saint Vincent and the Grenadines.

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

No interception by members of public

13. A 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.

Reporting obligation on illegal activity

14. If 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 a concerned party shall report the activity to a law enforcement official without delay.

Reporting obligation on actual illegal activity

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

### PART IV CONFIDENTIALITY IN RESPECT OF SUBSCRIBER

Strict control measures

16. A telecommunications provider shall 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.

Employee to execute agreement

- 17. (1) An employee of a telecommunications provider who has access to subscriber personal information or subscriber proprietary network information shall execute a non-disclosure agreement that is kept as part of that employee's permanent records.
- (2) Pursuant to sub-regulation (1) the terms of the agreement shall survive any reassignment of the employee to

other duties, the termination or departure of the employee from the employment of the telecommunications provider.

## Confidentiality of subscriber

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

## Permission to be first obtained

19. A telecommunications provider or publisher of subscriber and lists directories shall not list the subscriber's personal information in a telephone directory unless he first obtains the consent of the subscriber.

### Grounds for disclosure of proprietary network information

- 20. 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, unlawful use of, or subscription to such services; or
  - (b) provide the telecommunications services to which the proprietary customer has subscribed.

Dated the 29 day of January, 2002.

Dr. Jerrol Thompson Minister for Telecommunications