••

ATTACHMENT 9

NETWORK SECURITY

TABLE OF CONTENTS

Section **Page**

NETWORK SECURITY

I. Protection of Service and Property

GTE shall exercise the same degree of care to prevent harm or damage to AT&T, its employees, agents or customers, or their property as it employs to protect its own personnel, customers and property, etc. GTE, its employees, agents, or representatives agree to take reasonable and prudent steps to ensure the adequate protection of AT&T property and services, including, but not limited to:

A. Restricting access to AT&T equipment, support equipment, systems, tools and data, or spaces which contain or house AT&T equipment enclosures, to AT&T employees and other authorized non-AT&T personnel to the extent necessary to perform their specific job function. AT&T shall be responsible for maintaining security within its space (i.e., locking equipment enclosures, etc.). GTE will partition off collocation space and provide AT&T with a separate entrance to such space. If central office space does not permit partitioned space, GTE will escort AT&T personnel to and from AT&T equipment enclosures.

B. Furnishing to AT&T a current written list of GTE's employees who GTE authorizes to enter spaces which house or contain AT&T equipment or equipment enclosures, with samples of the identifying credentials to be carried by such persons.

C. Complying at all times with AT&T security and safety procedures and requirements, including but not limited to sign-in, identification, and escort requirements while in spaces which house or contain AT&T equipment or equipment enclosures and compliance with AT&T Corporate Security Instructions (CSIs) 1.01 "Admission to AT&T Premises", January 1987, CSI 1.10 "Physical Security For Shared Premises", Issue A, January 1987, and CSI 1.13 "Physical Security Criteria For Elements of the Network", Issue A, June 1987.

D. Allowing AT&T to inspect or observe spaces which house or contain AT&T equipment or equipment enclosures at any time and to furnish AT&T with all keys, entry codes, lock combinations, or other materials or information which may be needed to gain entry into any secured AT&T space.

E. Not using card access readers and devices that use cards which are encoded identically or mechanical coded locks on external doors or on internal doors to spaces which house AT&T equipment.

A. Insuring that the areas which house AT&T's equipment are adequately secured and monitored to prevent unauthorized entry.

B. Limiting the keys used in its keying systems for spaces which contain or house AT&T equipment or equipment enclosures to its employees and representatives to emergency access only.

AT&T shall further have the right to change locks where deemed necessary for the protection and security of such spaces.

A. Installing security studs in the hinge plates of doors having exposed hinges with removable pins if such doors lead to spaces which contain or house AT&T equipment or equipment enclosures.

B. Providing real-time notification to designated AT&T personnel to indicate an actual or attempted security breach in situations other than those in which AT&T has installed and monitors its own alarms.

C. Providing an acceptable back-up and recovery plan to be in the event of a system failure or emergency.

D. Installing controls:

- to disconnect a user for a pre-determined period of inactivity on authorized ports;
- to protect customer proprietary information; and,
- to databases to ensure both ongoing operational and update integrity.

m **Providing Logical Security:**

- securing all approved system and modem access through secured access.

· establishing access to or connection with a network element through a secure network or security gateway.

x complying with AT&T Corporate Security Instruction 3.03 "Computer Security Requirements," March 1993, and AT&T Network Security Requirements 4.0, March 1996.

In cases in which there is shared systems access to GTE systems, GTE will provide access controls to its system based upon GTE's internal security standards, which standards shall include, at minimum, traditional log in and password procedures. AT&T shall be responsible for AT&T control installation.

I. **Revenue Protection**

A. GTE shall make available to AT&T all present future fraud prevention or revenue protection features, including prevention, detection, or control functionality embedded within any of the network elements. These features include, but are not limited to screening codes, call blocking of international, 800, 900/976, and 700 numbers and the capability to require end-user entry of an authorization code for dial tone. GTE shall additionally provide partitioned access to fraud prevention, detection and control functionality within pertinent Operations Support Systems ("OSS").

B. Uncollectible or unbillable revenues resulting from, but not confined to, provisioning, maintenance, or signal network routing errors shall be the responsibility of the party causing such error.

A. Uncollectible or unbillable revenues resulting from the accidental or malicious alteration of software underlying Network Elements or their subtending operational support systems by unauthorized third parties shall be the responsibility of the party having administrative control of access to said Network Element or operational support system software.

B. GTE shall be responsible for any uncollectible or unbillable revenues resulting from the unauthorized physical attachment to loop facilities from the Main Distribution Frame up to and including the Network Interface Device, including clip-on fraud.

C. GTE shall provide quick/soft dial tone to allow only the completion of calls to termination points required by law.

I. **Law Enforcement Interface**

A. GTE shall provide seven day a week/ twenty-four hour a day installation and information retrieval pertaining to emergency traps, assistance involving emergency traces and emergency information retrieval on customer invoked CLASS services, including, without limitation, call traces requested by AT&T.

B. GTE shall provide all necessary assistance to facilitate the execution of wiretap or dialed number recorder orders from law enforcement authorities in emergency situations.

C. In nonemergency situations, GTE will advise the requesting law enforcement agency that the customer to be wire tapped is not a GTE customer but is an AT&T Customer. GTE will promptly notify AT&T of any court-ordered wiretap, dialed number recorder or trap which affects an AT&T customer.