COMPUTER CENTER PHYSICAL SECURITY AND DISASTER RECOVERY POLICY STATEMENT AND GENERAL INFORMATION

CONTENTS PAGE

1. GENERAL

1.01 This standard has been developed by a multicompany GUARDSMAN project team under the direction of AT&T Information Systems Technical Support and Standards. This standard is issued by the AT&T Director—Information Systems Planning and Support for implementation by Bell System Companies.

1.02 Whenever this section is reissued, the reason(s) for reissue will be listed in this paragraph.

1.03 As the Bell System becomes increasingly dependent on computer systems for its daily operation, the impact of a disruption of computer operations becomes increasingly severe, can affect service to the customers, and can delay the processing of information vital to the interest of the Bell System. In order to minimize the risk of an internal or external threat reducing the availability of a computer system, an effective physical security program should be developed. This program should be implemented in a manner appropriate to the impact of the computer system on the corporation.

1.04 A physical security program will reduce the risk of an interruption of the availability of a computer system, but will not entirely eliminate it. Therefore, an effective means of restoring the availability of a computer system is also required. Methods to restore the availability of a computer system (referred to as contingency planning and disaster recovery) should be implemented in a manner appropriate to the impact the loss of the availability would have on the corporation. This plan should be compatible with any other disaster recovery plans that may exist in the corporation.

1.05 The responsibility for establishing and maintaining an effective physical security and disaster recovery program rests with the organization responsible for operating the computer facility. A Corporate Computer Security Administration function should be established to ensure that the programs developed are compatible. The responsibilities of this function are defined in Section 007-590-300.

1.06 The establishment of a physical security and disaster recovery program is a Bell System standard. Guidelines on how to establish an effective program are contained in Sections 007-590-300 through 007-590-304.

1.07 This series of sections is designed to cover all computers, including minicomputers, used in the Bell System. This definition of scope is further defined in Section 007-590-301 (Identification of the Processing Environment).

2. POLICY STATEMENT

2.01 The policy of the Bell System is to provide reliable communications service to the public at a reasonable cost. In support of this policy the corporate assets must be protected. In the recent past, many corporate activities have been mechanized on computer systems. To be effective, these computer systems must have a high degree of availability. Therefore, a policy is established of physically securing against the loss of availability and providing for an effective means of recovery should a loss of availability occur. This policy should be implemented in a manner appropriate to the impact of the computer systems on the corporation.

Printed in U.S.A.

3. OVERVIEW

3.01 Sections 007-590-300 through 007-590-304 address the procedures and responsibilities necessary to establish an effective physical security and disaster recovery program. The sections are arranged in a manner similar to the work flow of establishing the program.

3.02 ***Administration (Section 007-590-300):*** This section describes the administration of a physical security and disaster recovery program. The job functions of a Corporate and Site Computer Security Administrator are defined as well as responsibilities throughout the corporation for administering the program. This section outlines the information contained in the remaining sections of this series.

3.03 ***Identification of the Processing Environment (Section 007-590-301):*** This section describes the environment that is to be protected and recovered. The purpose of this section is to limit the scope of this series of sections to the data processing segment of the Bell System. A glossary of terms is included in this section.

3.04 ***Impact Analysis (Section 007-590-302):*** Decisions to commit corporate resources to the security and recovery capabilities of a computer facility must be based on a realistic evaluation of the impact of that facility on the corporation. This section defines the methods for determining the impact as well as determining the weaknesses of the current security and recovery systems. This is done in four steps. They are:

(1) Evaluating application criticality and vulnerability

(2) Determining the physical assets of the environment

(3) Identifying potential threats to the environment

(4) Determining the vulnerability of that environment to internal and external threats.

The results of the impact analysis enable us to determine the degree of physical security required and to set priorities on the recovery of the applications.

3.05 ***Physical Security (Section 007-590-303):*** This section describes the various methods which can be employed in establishing a physical security program. It has been divided into three areas: protection by building design, protection by devices, and protection by procedures.

3.06 ***Contingency Planning and Disaster Recovery (Section 007-590-304):*** This section describes the methods and procedures for developing effective contingency and disaster recovery plans. It has been divided into three major areas: contingency planning, disaster recovery manuals, and disaster recovery operations.