DATA SECURITY ADMINISTRATION FOR COMPUTER SYSTEMS

DATA SECURITY PROGRAM

CONTENTS PAGE

1. GENERAL

1.01 This section has been developed by a multicompany project team under the direction of the GUARDSMAN Steering Committee. This standard is being issued by the Director—Data Systems of AT&T and has been agreed to by Bell Laboratories and AT&T. Any deviation from this standard by an Operating Telephone Company (OTC) is at its own risk.

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

1.03 The purpose of this section is to identify the activities and resources required to establish the Data Security Administration function.

2. DATA SECURITY PROGRAM COMMITMENT

2.01 Corporate commitment is vital to developing an effective data security program. The establishment of the data security program requires the following:

(a) Establishment of a data security policy

(b) Establishment of the Data Security Administration function

(c) Assignment of Data Security Administration responsibilities

(d) Initiation of the data security program which includes:

(1) Approval of a plan for the data security vulnerability study

(2) Cooperation of those functional areas whose support is needed in the program, ie, data systems, computer operations, auditing, security

(3) Acceptance by user departments of the requirement to define their data security needs

(4) Approval of budgets for the data security program

(5) Company-wide compliance with data security standards.

2.02 A corporate data security policy must emphasize the importance of data security throughout the organization. All departments, functions, and individuals must be aware of their data security responsibilities. Data security policy should be established in the following categories:

(a) Data gathering activities

(b) File contents

(c) Data storage and handling

(d) Data dissemination

(e) Data access

(f) Personnel

(g) Systems design

(h) Data system operations

(i) Auditing

(j) Data security administration.

3. DATA SECURITY ADMINISTRATION FUNCTION

3.01 The success of a data security program remains totally dependent upon the definition, assignment, and performance of the responsibilities for Data Security Administration. Specific individuals or organizational entities assigned these responsibilities may vary among companies; however, these functions must be performed effectively to prevent data security from existing in name only.

3.02 Organizations likely to be involved with data security include Data Base Administration, Data Communications Administration, Data Systems, Internal Auditing, Legal, and General Security. The designation of a Data Security Administration function to coordinate the effort of these and other groups is essential when addressing the problems of data security.

3.03 Data Security Administration responsibilities include:

(a) Development and maintenance of corporate standards relating to data security. Since much of the data under concern transcends organizational boundaries, a corporate standard appears more appropriate than standards applicable only at a departmental level.

(b) Analysis and classification of data. This effort will require the involvement of data systems, internal auditing, users, and other concerned areas for determining the security attributes of data associated with each system.

(c) Analysis and identification of data exposure. Since exposure relates to the computer environment as well as systems design, data system's application development groups may be involved in this effort.

(d) Evaluation of the application design and the selection of appropriate protective measures.

(e) Documentation of classification. A dictionary of data contained in data processing systems should be created, if it does not already exist, and must include some means of documenting the attributes and classifications associated with the data. Procedures should be established for updating and maintaining this dictionary to assure it reflects current security status of data.

(f) Analysis and selection of protective mechanisms appropriate to hardware and software configurations and corporate policy of the company. Protective mechanisms would include special physical security systems, special hardware features, software modules and features, utilities, manual procedures, etc.

(g) Continuing research into current state-of-the-art security and protective measures. Data security is a relatively new area of general concern in industry and as a result, concepts and facilities may be changing rapidly in this area. An ongoing effort is required to remain abreast of the current evolution in data security.

(h) Testing the effectiveness of protective measures. Periodic reviews of security classifications, exposure levels, and protective measures offer an ongoing assurance that the data security program remains effective.

(i) Review of system hardware and software changes or updates to evaluate their impact on data protective measures.

(j) Establishment of a data security educational program.

(k) Review of protective measure output such as logs, reports, etc.

4. DATA SECURITY VULNERABILITY STUDY

4.01 A project team composed of user groups, data systems, auditing, and security should conduct a company-wide data security vulnerability study. The team will require full-time participation for the duration of the vulnerability study.

4.02 A project plan should be developed to define the scope of the vulnerability study, the organizations affected, and a plan of action. Because of the level of technical detail required in the plan, ample expertise must be represented on the project team. The technical knowledge of the team may be supplemented by attending seminars, discussions with others who have attempted similar

projects, or by using the services of a consultant. The project team shall develop a proposal report to obtain management approval to continue with the data security vulnerability study.

4.03 The data security vulnerability study should focus on the data of the major computer applications of the company. These applications should be identified and priority assigned by how critical they are to the productivity of the company. A representative sample of these applications should be selected and its data reviewed using the guidelines defined in this section. The purpose of this initial study is to classify the data of the sample set and to assess their exposures to security threats. The vulnerability study report should list the reviewed applications and data, their exposures, and the potential loss to the Company if left unprotected. The report should include the project team recommendation for further action, estimated cost figures, staffing requirements, and other resources required for implementing the data security program.