DATA SECURITY ADMINISTRATION FOR COMPUTER SYSTEMS

DATA SECURITY IMPLEMENTATION AND ADMINISTRATION

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 Upon approval of the Data Security Program, those responsible for the Data Security Administration function should address development of:

(a) Adequate staffing of the Data Security Administration function.

(b) Data Security Standard—this may be developed in conjunction with other departments (data systems, internal auditing, security, users, and other concerned areas). The standard will define the data security responsibilities of each group.

(c) A plan for the implementation of data security protective measures in both new and existing applications.

(d) A data security educational program for all management, supervisory, and operating personnel in the data systems and user departments.

(e) A data security maintenance program with the assistance of all involved departments.

2. DATA SECURITY IMPLEMENTATION

2.01 Although data security is everyone's responsibility, the Data Security Administration function is responsible for the overall coordination of the design for data security. A person should be assigned to monitor data security aspects in all the phases of the system life cycle. This person should ensure that the system designers are aware of the need for data security and recommend the use of the procedures defined in this section.

2.02 A data security plan should be developed which will encompass existing computer applications as well as future applications either being developed or to be developed.

3. DATA SECURITY ACTIVITIES FOR EXISTING SYSTEMS

3.01 The Data Security Administration function is responsible for implementing the data security plan for existing systems and should start with a review of the vulnerability study. The application areas covered in the vulnerability study should be prioritized according to their vulnerability. A detailed analysis of the prioritized applications should be conducted to determine the cost/benefit of implementing the data security standard. Based on the results of the cost/benefit analysis, specific

protective measures should be selected for implementation.

4. DATA SECURITY ACTIVITIES DURING SYSTEM DESIGN

4.01 The following must be addressed by system designers and Data Security Administration:

(a) ***Definition Phase***

(1) Analyze all system data to determine its security attributes.

(2) Classify the system data.

(3) Document the attributes and classifications of all system data.

(4) Identify potential data security threats, exposures, etc.

(5) Decide whether the data protective measures will be required by the system.

(6) Define protective measures for the system.

(7) Define internal security measures to be utilized on the project (eg, security clearances of project personnel, protection and disposition of all project working documentation, etc).

(8) Evaluate data security measures in existing systems which interface with the new system and define changes which may be required.

(b) ***Design Phase***

(1) Specify detailed software security techniques.

(2) Perform Data Security Cost-Risk Analysis.

(3) Finalize and document the protective measures of the system.

(4) Develop detailed programming security procedures.

(5) Develop procedures for the delivery, retention, disposal of:

- Reports containing sensitive data
- Systems, programs, and documentation which process or reference sensitive data.

(6) Prepare a data security test plan to certify that protective measures are properly implemented and effective.

(c) ***Implementation and Conversion Phases***

(1) Implement selected protective measures.

(2) Execute the data security test plan.

(3) Review test results and iterate as necessary.

(d) ***Performance Review Phase:*** The system security results should be reviewed with all involved departments (data systems, operations, internal auditing, and users), and the protective measures modified as appropriate to provide the security specified in the system design.

5. DETECTION OF DATA SECURITY VIOLATIONS

5.01 Protective measures are designed to prevent and detect unauthorized access or usage of system data. The detection of attempted or actual violations, whether signaled immediately or recorded for later analysis, must trigger follow-up action. Detection of violations is an indication that the protective measures are working but does not assure that undetected violations have not occurred. The purpose of reviewing the protective measure output is to detect security breaches.

5.02 Reviews of protective measure output on a regular, periodic, and special basis.

(a) Regular reviews of:

(1) Reports of violations of authorization tables, password tables

(2) Standards violations

(3) Procedural violations at remote terminals

(4) Unauthorized access to specific files.

(b) Periodic reviews of:

(1) Console operator logs

(2) File activity

(3) System and program changes

(4) Environmental, operational, and personnel changes

(5) Legislative, social, and legal actions affecting data security.

(c) Special reviews of information identifying possible data security breaches.

5.03 Violations of data security are either accidental or deliberate. Examples of these violation types are listed below:

(a) ***Accidental Violations:*** The consequences of accidental disclosure of sensitive information are as serious as those resulting from a deliberate violation. Accidental disclosure of data could result from:

(1) Hardware failure (misrouting of information)

(2) Software errors (system crashes, poorly designed or inaccurate programs)

(3) User errors (unplanned usage)

(4) Operational errors (mounting wrong tape or disk pack)

(5) Communication errors (improper switching and crosstalk)

(6) Procedural errors (distributing sensitive reports to the wrong person or improper identification of sensitive data).

(b) ***Deliberate Violations:*** Deliberate violations imply preconceived objectives such as gaining access to file information, altering or destroying files, obtaining free use of system resources, etc. Examples include:

(1) Electromagnetic pickup

(2) Wire tapping

(3) Perusal of discarded material

(4) Browsing through files

(5) Masquerading as legitimate program

(6) Specially planted software entry points.

5.04 Procedures for processing detected violations are outlined below:

(a) Information collection regarding detected security violations would include:

(1) Identification of terminal or location of violation

(2) Identification of person or system function involved

(3) Date and time of violation

(4) File, data base, or data element involved

(5) Program involved.

(b) Analysis of the violation to determine:

(1) The seriousness of the violation.

(2) The state of the violation (imminent, in progress, or past).

(3) Type of violation (accidental or deliberate).

(4) The priority afforded the violation, ie, is immediate action necessary or are other violations more serious?

(5) The procedures required to counteract or control the violation.

(6) Persons responsible for the violation.

(c) Action should be taken to:

(1) Notify responsible parties (by alarm, phone, etc) that a violation is imminent, in progress, or has occurred.

(2) Start contingency actions to either stop or prevent the violation.

(3) Start corrective actions to ensure that the security of the system is maintained at an adequate level.

(4) Notify responsible parties of the identity of personnel involved in the violation for appropriate disciplinary or legal action.

(d) Violation History—Historical information concerning the violation should be retained to determined patterns. Corrective actions should also be recorded to ensure that the violation has been successfully addressed. This information would be used to evaluate the adequacy of the protective measures.

5.05 Undetected violations are those not detected by existing protective measures but which come to light through mistakes of the violators, through external feedback, or happenstance occurrences. Assessment of damage done by these violations is different because they may have been in existence for a long period and could have caused considerable harm. The same actions would be taken for undetected violations as previously outlined for the detected violations. In addition, the protective measures presently in use would have to be reviewed and changed to prevent the now detected violation from occurring again.

6. MAINTENANCE OF DATA SECURITY PROGRAM

6.01 Protective measures, procedures, etc, should be monitored regularly. Monitoring involves:

(a) ***Tests of Protective Measures:*** The tests should not merely validate the existence of protective measures but should make conscious efforts to breach the system's security.

(b) ***Reviews of Data Security Procedures:*** These reviews include:

(1) Current technical effectiveness of security measures

(2) Current effectiveness of security tests

(3) Continuing validity of data classification and the criteria used for that classification

(4) Current cost effectiveness of protective measures

(5) Adequacy of training in data security standards and techniques.