DATA SECURITY ADMINISTRATION FOR COMPUTER SYSTEMS

PROTECTIVE MEASURES

CONTENTS PAGE

1. GENERAL 1

2. PROTECTIVE MEASURES 2

3. ACCESS RELATED PROTECTIVE MEASURES 4

4. USAGE RELATED PROTECTIVE MEASURES 4

LIST OF ATTACHMENTS . . . . .

Attachment I—Protective Measures Worksheets Instructions I-1

Attachment II—Protective Measures—Access Exposure Worksheet . . . II-1

Attachment III—Protective Measures—Usage Exposure Worksheet . . . III-1

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 Data protective measures are the positive acts taken by human or machine to lessen the risk of accidental or unauthorized disclosure, modification, or destruction of data resulting from the various exposures to which the data is subjected.

1.04 Exposure is the degree of relative availability of the data in the environment in which it is used. The design of the system, physical location, hardware, software, and the means of accessing it will contribute to its exposure.

1.05 While a detailed list of real or potential exposures may be almost limitless, exposures can be grouped into two major categories: usage related and access related. Usage exposures are those relating to the destruction or modification of data or the deterioration of its integrity. Access exposures are those relating to unauthorized access or disclosure of data.

2. PROTECTIVE MEASURES

2.01 Protective measures are generally designed to address either access or usage exposures. The protective measures identified in Parts 3 and 4 have been separated into access and usage related categories. Within each of these exposure categories, the protective measures have been divided into three groups representing measures appropriate for minimum, moderate, and high risk. Implementation of higher risk protective measures assumes that substantial portions of the lower risk protective measures, appropriate to the data in question, have also been implemented.

2.02 Assessment of the minimum protective measure level is somewhat subjective and may require further economic analysis as defined in Section 007-301-205. As a minimum, within each of the exposure categories (usage and access), data with only one attribute requires it to be considered as low risk. Data with two attributes requires it to be considered as moderate risk. Data with more than two attributes requires it to be considered high risk. In any case, obvious overriding considerations can cause data to be raised to higher risk levels. Attachment I illustrates the process of selecting protective measures.

3. ACCESS RELATED PROTECTIVE MEASURES

3.01 Protective measures for access related exposures are directed at assuring that data is accessed only by authorized persons or programs. A policy of making data available on a need-to-know basis and security clearances for individuals appropriate to the data with which they work are generalized approaches in access control. Specific access related protective measures are described in this part.

MINIMUM RISK

3.02 ***Physical Security:*** Physical security encompasses such items as locking cabinets, guard stations, identification badges, terminal key locks, etc. A more complete list of physical security measures is contained in Comptroller's Letter M-471.

3.03 ***Data Only Accessible by Computer:*** Data stored on a machine-readable medium requires not only physical access to the media but also access to computers and programs to translate the data into a format intelligible to humans.

3.04 ***Program and Procedure Libraries Control:*** All executable programs and procedures reside in authorized libraries stored in a computer. These libraries must be maintained by a librarian with entry and removal only through supervisory approval with proper authorization.

3.05 ***User Identification:*** Systems that can be accessed remotely require some means of identifying a terminal and the person using that terminal. Personal identification can be accomplished by establishing identifying criteria for the terminals and the users. These identifiers can be changed periodically or when an occasion calls for such changes. Terminal identification can be accomplished by a terminal generated answerback code.

3.06 ***Off-line Storage:*** Data, when not required for authorized processing, are maintained in a nonaccessible state. This may be implemented in varying degrees such as, access logically inhibited, physically removed from the device, or physically in a library. Reference M-471, regarding Physical Security.

3.07 ***Devices with Write Suppression:*** Many peripheral devices such as disk drives and tape drives have the capability of suppressing the ability to write on files mounted on them via switches, file protect rings, etc. Many CRT devices have the ability to selectively suppress the update of fields on their screen format, generally under software control. Write suppression affords protection to data which can be accessed but not updated.

3.08 ***Distribution Control:*** Physical distribution of input or output media should be conducted in a controlled environment by use of in-house mail facilities or special courier services. A continuous distribution logging system increases the security of output distribution.

3.09 ***Disposal Control:*** Special contracts with waste collectors should include a nondisclosure clause which will assure that outputs are disposed of in a manner consistent with minimum security requirements. Reference General Letter 77-01-152, ***Revised Guidelines and Procedures for Safeguarding Proprietary Information.*** Not only hardcopy output but also carbon paper, ribbons, microfiche, microfilm, and other media should be subject to controlled disposal.

MODERATE RISK

3.10 ***Separation of Responsibilities:*** A method of protection is to separate responsibilities so that collusion of two or more persons is necessary to compromise the security of data. Examples of separation of responsibilities to effect data security are: production programs and data from testing programs and data, design from programming, and computer operation from job setup operation.

3.11 ***User Restriction:*** A remote user who has signed onto a system in an authorized manner should only be permitted to use limited system resources or access restricted sets of data. Some combination of user identification, physical location, transaction identification, data base identification, or time of day can be used to further restrict capability to access certain data. This protective measure may partially be supplied by the system software but frequently must be supplemented by locally written programs.

3.12 ***Terminal Access Control:*** Terminal access control provides the ability to uniquely identify and selectively restrict terminal access to

the computer system. The switched communications network affords any terminal the capability of accessing the computer. The terminal call-back technique will control access as follows: after originating an initial contact with the computer system, the terminal is disconnected. The computer system reestablishes the connection by dialing the terminal's assigned telephone number, thus providing verification of the terminal's location and identification. Both host computer and terminal require hardware features to permit this type of communication Another alternative is to use private line facilities rather than the switched network which will restrict the number and location of terminals that have access to the computer.

3.13 ***Controlled Resource Sharing:*** Computer mainframes or shared peripheral devices can be partially isolated on the basis of common security levels. For example, high security programs may be restricted to run on only one processor in a multiple computer operation, or disk files containing sensitive data may be restricted to a subpool of the available disk spindles.

3.14 ***Entrapment:*** System components whose sole purpose is to expose security breaches. Fictitious files, never accessed by the legitimate production system, may be embedded into production systems. Output containing elements of this fictitious data would indicate a security breach.

3.15 ***Terminal Activity Monitors:*** Deviations from anticipated activity (transaction types, volumes, schedules, etc) of network links and specific terminals can be detected by analysis of a terminal log and comparison to expected acceptable values. Deviations can then be further investigated for security violations.

3.16 ***Copy Control:*** Data copies should be restricted to a minimum number in order to increase the effectiveness of other protective measures. At input time, direct entry of the data from the source into the system would be preferable to creation of an interim copy(s) of the data. During system processing, intermediate file creation may be minimized by use of a direct access file with minimum file backup. Hardcopy output including program or system dumps can be minimized by use of single part paper and special handling instructions which restrict reproduction (Reference: General Letter 77-01-152, ***Revised Guidelines and Procedures for Safeguarding Proprietary Information).*** Finally, this control should be extended to remote hardcopy devices by elimination of the hardcopy device or requiring system authorization prior to printing.

3.17 ***Security Violation Logs:*** Unsuccessful attempts at terminal sign-on, attempts to use invalid transaction codes, etc, should be recorded on system logs. This log should be used to investigate attempted penetrations and to measure the effectiveness of access controls.

3.18 ***Program/Procedure Library Review:*** Regular reviews of program and procedure libraries will identify unauthorized programs or files.

HIGH RISK

3.19 ***Dedicated System Resources:*** Data should be isolated from other data and processes by various levels of dedicated facilities. This may be accomplished by dedicating storage devices with single access paths, dedicating tape or disk storage media, or dedicating an entire computer system.

3.20 ***Network Security Verification:*** Wire taps and piggybacks usually occur at the host computer for switched lines and at either end for private lines. Periodic physical and electronic inspection of communication facilities should be conducted to detect unauthorized attachments.

3.21 ***Cryptography:*** Cryptography is used to make the data unintelligible to other than the authorized users. Most practical cryptographic controls rely on enciphering, a substitution of one or more alphanumeric characters (or bits) of enciphered text for each character (or bit) of plain text. Enciphering can be accomplished by hardware devices which is the classic means for securing data transfer over communications lines. Data accessed within the confines of a computer system can also be enciphered by use of software algorithms and data keys.

3.22 ***Program Lockout:*** A given collection of data carries with it the identification of specific programs that may access it. Attempts by any program other than this select group to gain access to such data is inhibited and logged as a security violation. This control would ideally even inhibit use of general purpose operating system

utilities, if they were not on an authorized list. Implementation of this facility may require local programming.

3.23 ***Erasure of Stored Data:*** As soon as stored or recorded data is no longer required, the physical media on which it resides is erased to prevent access.

(a) ***Temporary Storage:*** Data contained on temporary storage, eg, core, disk, tape, and drum should be erased or overwritten by the program or the operating system.

(b) ***Remote Devices:*** Data residing in remote terminal buffers should be erased or overwritten by the operating system.

(c) ***Permanent Storage:*** Data residing on permanent storage should be overwritten with unintelligible data or erased by total magnetic neutralization (degauss).

3.24 ***Data Access Verification:*** Data access verification ensures that the access to data required by a system is intact and viable. Programs may be written to check catalogs of data files against physical files, validity of the volume table of contents on disk packs, correct index chaining on data bases, etc. Exceptions are noted for further investigation. In some cases, a file could be marked as unusable pending completion of such an investigation.

4. USAGE RELATED PROTECTIVE MEASURES

4.01 Protective measures for usage related exposures address the requirements to assure and maintain validity and to provide for the continued existence and recoverability of the data.

MINIMUM RISK

4.02 ***Physical Protective Controls:*** Environmental controls to maintain temperature and humidity, isolate from electromagnetic radiation, prevent or suppress fires, provide physical security, etc, fall in this category. A more exhaustive list of such protective measures can be found in M-Letter 471.

4.03 ***Error Correcting Hardware:*** Most computer and peripheral devices have some means of detecting errors generated during electronic transfer of data. Depending on the level of design sophistication, many hardware devices not only detect but also correct errors.

4.04 ***Certification Testing:*** A thorough and concise test plan based on the specifications of the system should be established. The system tests prove the correctness of a system in processing data according to specifications. Regression testing demonstrates the validity of the old system with newly inserted changes. Invalid data is used in a conscious effort to breach controls and edits. Reference Comptroller's M-Letter 447.

4.05 ***Batch Controls:*** Where data are assembled in batches for input, separate control records should be generated to assure data is not lost in transit or processing. In addition to batch identification and item count, such control records should also include source or destination identification, batch totals on key numeric fields in the input records, hash totals, and any other appropriate control criteria.

4.06 ***Intertask Processing Controls:*** Where data are processed through a series of sequential job steps or proceed through a periodic cycle of programs, controls are established for the entire job or cycle. These controls are similar in content to batch controls and should include time, date, condition codes, record counts, key field totals, hash totals, source, destination, and any appropriate control criteria.

4.07 ***Accuracy Controls:*** Accuracy controls are necessary for protection of data. The subject of accuracy controls is dealt with in detail. Accuracy controls that relate to data security include but are not limited to:

(a) ***Format Edits:*** Input data are subjected to such tests as alpha/numeric/blank column, field signs, reasonable values, sequence checks, etc, to assure the initial integrity of data upon entry to a system.

(b) ***Validity Edits:*** Where data can have anticipated values or ranges of values, known on the basis of design or history, data should be examined to identify deviations from these anticipated values.

(c) ***Field Fillers:*** A data field of fixed length but capable of variable length data content

may require filler characters in unused data positions to assure they are not inadvertently filled with invalid data. Examples might include leading zeros in keypunch card fields and asterisks preceding dollar amounts on checks.

4.08 ***Simultaneous Use Control:*** Hardware devices frequently have features which prevent more than one program from simultaneously using the data residing on that device. Most operating system software and data base management systems have software safeguards which can control concurrent access to the same data.

4.09 ***Secondary Data Storage:*** Copies of data are physically stored in more than one location which normally are geographically separated. Reference Comptroller's Letter M-471, regarding Physical Security.

4.10 ***Off-Line Storage:*** Data, when not required for authorized processing, are maintained in a nonaccessible state. This may be implemented in varying degrees such as, access logically inhibited, physically removed from the storage device, or physically in a library. Reference Comptroller's Letter M-471, regarding Physical Security.

MODERATE RISK

4.11 ***Positive Input Response:*** Any data received from an external source must have a positive acknowledgment of its receipt returned to the originator.

4.12 ***Self-Checking Data:*** Data requiring extreme accuracy should be subjected to processing algorithms to create check digits or fields. Each time such data is processed the algorithm is used to verify that its content still generates the proper check data.

4.13 ***Validation Measure:*** Validation facilities should be implemented as part of the system to assure proper system functioning. These facilities will allow validating data to be processed by the production system throughout its life to assure that it is processing accurately and as defined. Errors recognized from this validation process are indicative of those inherent in the production system.

4.14 ***Intent Control:*** A program is authorized to perform only specific functions on a given collection of data, eg, delete, replace, and insert. Unauthorized functions are inhibited and attempts to use unauthorized functions are logged for further investigation. Data base management systems provide varying levels of intent control but supplementary functions may be required.

4.15 ***File Activity Monitoring:*** Information about accesses to data such as program identification, terminal identification, user identification, date, and time are recorded. Interrogation of the log can be employed to identify situations such as unauthorized or unusual accesses.

4.16 ***Data Activity Logs:*** Activity logs contain copies of transactions, images of data before and after changes, or some combination of the three. These logs facilitate restoration of data or reprocessing of transactions to reestablish data to some processing point.

4.17 ***Change Logs:*** Change activity logs contain information covering all changes to hardware, software, computer center operating environment, and procedures. These logs assist in pinpointing errors introduced with change and facilitate recovery procedures.

4.18 ***Data Copies:*** Copies of files are made at logical breakpoints in a process, eg, end of cycle, end of day. These copies are used to restore data to its condition at the point where the copy was made.

4.19 ***Manual Verification:*** Computer processing is simulated by comparable manual processing of the same input data with the end results compared. Where the volume of data makes total manual verification impractical, scientific samples can be extracted to prove the accuracy of the processing to within acceptable limits.

HIGH RISK

4.20 ***Delayed Update:*** Delayed updating of data should be implemented in any on-line system when performance constraints restrict complete editing or when control deficiencies inherent in system control software cannot be tolerated. (High Risk)

4.21 ***Double Processing:*** The objective of this measure is to assure proper functioning of hardware and/or software by processing the input data two or more times and then comparing the results. This process may use different programs, different reference data, different hardware, or any combination of these system elements. However, the logical processing and outputs should be identical. This may take place in parallel or in different time frames. (High Risk)

PROTECTIVE MEASURES WORKSHEETS INSTRUCTIONS

The protective measures worksheets are provided as a documentation aid for the Data Security Administration function.

INSTRUCTIONS

(1) References the ***Data Attribute and Classification Worksheet*** (see Attachment I of Section 007-301-203). If there is a number greater than zero in the ***A*** column for each data item entry, include that data entry on the ***Protective Measures—Access Exposure Worksheet.***

If there is a number greater than zero in the ***U*** column for a data entry, include that data entry on the ***Protective Measures—Usage Exposure Worksheet.***

(2) For each data entry on either worksheet, enter under the appropriate protective measure column either:

X—if that protective measure already exists in the system or environment.

R—if that protective measure does not already exist but is required.

I—if that protective measure is inappropriate for the data element.

(3) Every protective measure column under the appropriate risk level (***U*** or ***A*** value) must have an entry of X, R, or I.

(4) Entries under protective measure columns at higher risk levels are optional.

PROTECTIVE MEASURES—ACCESS EXPOSURE WORKSHEET

Application _____

Data Identification	Minimum Risk (A = 1)								Moderate Risk (A = 2)									High Risk (A > 2)					
	1 Physical Security (3.02)	2 Data only Accessible by Computer (3.03)	3 Program and Procedure Libraries Control (3.04)	4 User Identification (3.05)	5 Off-Line Storage (3.06)	6 Devices with Write Suppression (3.07)	7 Distribution Control (3.08)	8 Disposal Control (3.09)	1 Separation of Responsibilities (3.10)	2 User Restriction (3.11)	3 Terminal Access Control (3.12)	4 Controlled Resource Sharing (3.13)	5 Entrapment (3.14)	6 Terminal Activity Monitors (3.15)	7 Copy Control (3.16)	8 Security Violation Logs (3.17)	9 Program/Procedure Library Review (3.18)	1 Dedicated System Resources (3.19)	2 Network Security Verification (3.20)	3 Cryptography (3.21)	4 Program Lockout (3.220	5 Erasure of Stored Data (3.23)	6 Data Access Verification (3.24)

Prepared By: _____ Date: _____ Approved By: _____ Date: _____

PROTECTIVE MEASURES—USAGE EXPOSURE WORKSHEET

Application _____

Data Identification	Minimum Risk (U = 1)									Moderate Risk (U = 2)									Hig Risk (U > 2)	
	1 Physical Protective Controls (4.02)	2 Error Correcting Hardware (4.03)	3 Certification Testing (4.03)	4 Batch Controls (4.05)	5 Intertask Processing Controls (4.06)	6 Accuracy Controls (4.07)	7 Simultaneous Use Control (4.08)	8 Secondary Data Storage (4.09)	9 Off-Line Storage (4.10)	1 Positive Input Response (4.11)	2 Self-Checking Data (4.12)	3 Validation Measure (4.13)	4 Intent Control (4.14)	5 File Activity Monitoring (4.15)	6 Data Activity Logs (4.16)	7 Change Logs (4.17)	8 Data Copies (4.18)	9 Manual Verification (4.19)	1 Delayed Update (4.20)	2 Duplicate Processing (4.21)

Prepared By: _____ Date: _____ Approved By: _____ Date: _____