COMPUTER SECURITY - DATA COMMUNICATION NETWORKS

CONTENTS PAGE

SECURITY - DATA COMMUNICATIONS

CONTENTS PAGE

SECURITY - DATA COMMUNICATIONS

CONTENTS PAGE

APPENDICES

1. PURPOSE AND SCOPE

A. Introduction To Data Communication Networks

1.01 DCN SECURITY RATIONALE: Integrity, availability, and confidentiality of Data Communication Networks (DCN) are major concerns of SWBT. Corruption, denial, or theft of communication services and network resources can disrupt critical network services and severely impact customer confidence. Data communication networks are increasingly in need of protection from a growing community of sophisticated attackers. Unless they are adequately protected, customers will increasingly distrust them and SWBT will not be able to provide reliable services when they are needed. The proliferation of computer systems and the rapid growth in their electronic interconnections has led to serious concern about the safety of SWBT information from theft, alteration, unauthorized disclosure, and intentional or accidental destruction. The SWBT data communication network must not be considered immune to these threats.

Technical and management standards to protect this environment are documented in this practice.

1.02 DCN COMPONENTS: Data communication networks have many components: network software and equipment comprising servers, modems, gateways, routers, and bridges. Within SWBT, a DCN or "network" includes the following:

- Wide Area Network (WAN)
- Integrated Communication Network (ICN)
- Virtual Telecommunications Access Method (VTAM)
- LAN Integrated Network Communication System (LINCS)
- Token Ring LAN
- CO-LAN/Datakit
- MicroLink II Public Packet Switch Network (PPSN)
- Private Lines

1.03 PROTECTING OTHER SWBT RESOURCES: This document does not address individual security issues for Network Elements, Operating Systems, various hosts, applications or application program interfaces, physical security and disaster recovery. For these areas, see the following practices:

- Off-Premise Storage, SW 007-590-904
- Physical Security-Computer Facilities, SW 007-590-905

- Disaster Recovery, SW 007-590-906
- Computer Security-Mainframes, SW 007-590-907
- Computer Security-UNIX Platforms, SW 007-590-908
- Micro-Computer Security Procedures, SW 007-590-911
- Guidelines for Developing Application Security, SW 007-590-912
- Computer Security-Network Elements, SW 007-590-913 (to be issued in 1994)

1.04 COMPLIANCE PROCESS: In an idealized world, host security would be sufficient to guard against covert attacks and intrusions. However, at least for the near-term, it is generally accepted that relying on host security is too problematical; there are too many hosts, too many different kinds of hosts, too many different sets of user needs, and too few qualified administrators. The installation of host security controls and procedures, while giving the appearance of compliance, may not produce required results. Satisfactory compliance is achieved when host and/or network controls are effectively used to:

- Secure individual systems (Hosts and Gateways);
- Limit network access;
- Isolate or quarantine critical systems;
- Effectively communicate prevention policies and procedures
- Monitor security.

1.05 TECHNOLOGY AND INDIVIDUALS: Technology is constantly changing and information protection measures must keep pace with these changes. However, security technology is ***NOT*** a panacea for problems in information access or control. SWBT's experiences in this area fully support what industry and academic experts say about the importance of individuals:

> ***"Protecting information depends primarily on individual employee ACTIONS, NOT on technical fixes"***

B. SWBT Policies on Protecting Resources

1.06 PERSONNEL COVERED: All employees of SWBT ***MUST*** comply with the policies and procedures in this practice. This includes permanent and

temporary employees as well as designated Company agents. It is Company policy that:

> ***"Fulfilling SWBT Protection of Electronic Information responsibilities is MANDATORY and a condition of continued employment."***

1.07 RULE OF LEAST PRIVILEGE: The network ***MUST*** have the ability to control access to commands that affect its configuration, routing, flow control, and any other features that determines how it handles traffic. Only authorized administrative users can be allowed access to network software and data that is part of or controlled by the network. In accordance with OP113:

> ***"A person will ONLY be given system access to information that he is AUTHORIZED to receive and which he NEEDS to perform his job duties."***

1.08 ELECTRONIC PRIVACY POLICY: The following policy has been established as the SWBT standard for all electronic systems and data:

> ***"Southwestern Bell Telephone Company (SWBT) electronic and computer resources are provided for the transaction of Company business, and no personal use is intended or approved. The Company may exercise at any time its right to inspect, record, and/or remove all information contained therein, and take appropriate action should unauthorized or improper usage be discovered. The policy of the Company with respect to electronic information (this includes but is not limited to programs, data bases, files, E-mail records) is no different from the policy concerning paper records: i.e., while the Company at all times retains the right to inspect, record, and/or remove all information made or kept by employees utilizing Company resources, such inspection, recording, or removing takes place only on the basis of Company need. Need includes but is not limited to management's determination that reasonable cause exists for belief that laws, Company policies or management directives have been, are being or may be broken or violated."***

1.09 ENCRYPTION KEYS: Encryption keys - Sensitive or critical data and/or files ***MAY*** need to be maintained or transmitted in an encrypted format. While encryption keys ***MUST*** be kept from unauthorized disclosure, they ***MUST*** be provided to Asset Protection or management upon request.

C. Terminology and Definitions

1.10 HOW TERMINOLOGY IS USED: When first used, significant items will be defined and are cross-referenced in Appendix 2, Information Security Index. Definitions are not intended to be exact technical descriptions, but rather are general descriptions for the use of SWBT employees in implementing security in an inter-networked environment.

1.11 SECURITY TERMINOLOGY: The following are definitions of some of the basic concepts used in this document.

a. Data - In accordance with OP113, any information in an electronic format whether stored, processed, or transmitted.

b. Guidelines - Rules which are highly recommended but because of an overriding concern (too costly, interferes with the business, etc.) might not be implemented, are recognized by the use of the capitalized words ***"SHOULD"*** or ***"MAY."*** Circumstances which do not meet the recommended guidelines ***MUST*** be documented and justified.

c. Standards - Rules which ***MUST*** be followed and are recognized by the use of the capitalized words ***"MUST"*** or ***"SHALL."***

1.12 NETWORK SECURITY THREATS: A network security threat is a condition or action, accidental or deliberate, that might compromise the quality or functionality of network services. These threats may be malicious or mischievous and can be categorized by the following:

a. Masquerade - Where one user or system tries to impersonate another in order to gain unauthorized access with all the privileges of the mimicked identifier.

b. Unauthorized Access - Occurs as a result of a successful masquerade or through defeat or circumvention of access controls, such as password decoding.

c. Disclosure - Information, either deliberately or accidentally, could be disclosed without authorization. Information broadcast throughout the network in clear text is susceptible to disclosure.

d. Modification - Data, software and messages could be modified surreptitiously by unauthorized users resulting in compromised integrity.

e. Denial of Service - An attack that modifies routing information or removes equipment from service could render equipment inoperable or force the equipment to operate in a degraded state.

f. Theft of Service - An attack to circumvent the tracking and charging mechanisms involved in billing through fraudulent means.

D. Practice Administration

1.13 SW910 MAINTENANCE: SW 007-590-910 (SW910) is maintained by the Computer Security Administration Group (CSAG) in Information Services. Updates are correlated to releases of Operating Practice No. 113 (OP113), Protection of Electronic Information. New releases of this practice will be filed with the Company documentation coordinators, mailed to each State and Interdepartmental Security Forum (ISF) representative and will be available on the STAIRS and TDIS electronic documentation systems.

1.14 SW910 QUESTIONS: Questions or comments on SW910 should be referred to the CSAG on the PHONE system (BLUE pages option) under Computer Security Administration Group (CSAG), by phone at 314 235-2935, or by e-mail to csag@isoa.

2. SECURITY RESPONSIBILITIES

A. Organizational

2.01 INTERDEPARTMENTAL SECURITY FORUM (ISF): The Interdepartmental Security Forum (ISF) is responsible for company policies and procedures for the protection of Electronic Information (EI). ISF membership includes at least one representative from each SWBT sixth level organization and various experts from relevant technical areas. The ISF develops, documents, and approves EI policies, standards, and practices. It also

assists in the evaluation of actual or suspected unauthorized access events. A list of the current ISF membership is available on the company electronic documentation systems, STAIRS and TDIS, as part of the security listing. Contact can also be made via E-mail to isf@isoa.

B. Individual & Functional

2.02 DCN SYSTEM ADMINISTRATOR: The System Administrator for a DCN, is the SWBT employee(s) who manage the computer equipment used to support DCN operation. Generally, this function includes resolution of hardware questions and various generic and automated processes such as software backups.

2.03 DCN SECURITY ADMINISTRATOR: Application and/or system security may be an additional duty for the System Administrator. However, for all applications, systems, and DCNs, a SWBT manager(s) ***MUST*** clearly be assigned the appropriate security responsibilities. In the case of a DCN, the Security Administrator has the responsibility of installing and maintaining the security elements for that DCN. In addition, the security administrator ***MUST*** conduct an annual trust-level certification of his/her particular network segment. This person(s) ***MUST*** be trained in the particular security measures for the assigned platform and ***MUST*** be registered with the ISF by completing Appendix 5 of OP113 and returning it to the organizational ISF representative.

2.04 RISK ANALYSIS: During development, the DCN Security Administrator and platform specialists decide which security elements are required for a given DCN by performing a risk analysis. This is the process of balancing the cost of protection against the risk of exposure. When they are at almost the same point, security measures are properly balanced and prudent. It is necessary on a case-by-case basis to decide if more is being spent on security than it is worth, or if too little is being spent and the Company is imprudently being exposed. This involves putting in place the necessary measures so that a security event will not occur at all, or so that a security event becomes much less likely or costly. The ISF can provide specific assistance on performing a risk analysis.

3. SECURITY REQUIREMENTS

A. Integrity Controls - Hardware and Physical Environments

3.01 PHYSICAL ACCESS CONTROLS-GENERAL: Specific procedures and associated physical access controls for raised-floor environments are

described in SW 007-590-905 (SW905), Computer Facility Physical Security. For environments other than raised floor, see SW 007-590-911 (SW911), Micro/Personal Computer Security.

3.02 SPECIFIC DCN COMPONENTS: Network devices such as terminal servers, routers, bridges, etc., ***MUST*** be treated as computers and placed in secure locations. Network cables, although less of an immediate security concern than devices, ***SHOULD*** be placed in either secure, or readily inaccessible locations. With the recent proliferation of portable network analyzers and testers, anyone with access to an Ethernet cable has the capability to scan network traffic.

3.03 HARDWARE TRACKING: Hardware ***MUST*** be identified in accordance with Company practices and tracked by the responsible organization to assure proper utilization of Company resources.

3.04 EARTHQUAKE PROTECTION: Areas vulnerable to earthquake may require special procedures and protection materials. These areas and special requirements are documented in SW905.

3.05 ENVIRONMENTAL REVIEW: An annual environmental review ***MUST*** be performed and documented as described in SW905 and SW911.

B. Integrity Controls - Software and Data

3.06 CHANGE CONTROL PROCESS: The initial installation and each update to software ***SHOULD*** be performed in a manner that does not compromise security or leave the Company open to software licensing liabilities.

a. All DCN software changes ***MUST*** be documented and reviewed to determine that security has not been compromised. Foreign or public-domain code/programs ***MUST NOT*** be loaded unless they have been evaluated and approved against unauthorized changes (e.g., Trojan Horse), virus contamination, etc.

b. Proof of Company ownership of all DCN software ***MUST*** be available through the purchasing organization or from the System Administrator. Unless authorized, employees or authorized Company agents ***MUST NOT*** copy software developed or purchased by the Company, use copied software, or use code-breaking devices which allow copy-protected software to be used.

c. Employees and authorized Company agents ***MUST NOT*** develop, copy or use any program or code which circumvents or bypasses system security or privilege mechanisms or distorts accountability or audit mechanisms.

3.07 BACKUP PROCESS: Procedures ***MUST*** be documented and used that provide for the copying and protection of DCN application and system software. These master copies ***MUST*** be used for recovery in the case of accidental or intentional loss or corruption of the software. Backup data ***MUST*** be created and maintained in accordance with Operating Procedure No. 47 (OP47), Document Retention. In addition, to prevent unauthorized access to SWBT data and software, a storage device which leaves the control of SWBT ***MUST*** have all data removed (e.g., overwritten or the device destroyed).

C. Access Controls - Guidelines and Models

3.08 SWBT SECURITY MODELS: The security of electronic information passed from point A to point B over an electronic transport ***MUST*** be maintained at all times. SWBT has developed the Security Domain and Trust Level models to simplify the planning and management of security relationships during a session. In the Security Domain model, elements from three areas or domains, the "User", "Transport", and "Data" are connected to create a session. The session's security requirements are evaluated based on the Trust Level model to define a balanced and standard set of security arrangements between users and SWBT systems. The security domain and trust level models reflect the strategic direction that SWBT is taking in regard to insuring data integrity. More detailed information concerning these models may be found in OP113, paragraphs 4.302 through 4.305.

3.09 SECURITY DOMAIN MODEL: In this model, elements from three areas (domains) are combined to allow a user to interact with a system which contains desired data.

a. User Domain: The physical location and device combination from which the user initially requests access to Company resources (i.e., a terminal or PC in a Company location, a personal PC in an employee's home, etc.).

b. Transport Domain: The Company or public networks used to interconnect the User Domain to the system containing the data or services being requested (i.e., VTAM, a SWBT LAN, etc.).

c. Data Domain: The Company system or application containing the SWBT data or services which is requested during a session (i.e., SORD, LMOS, EVP, etc.).

3.10 TRUST LEVEL MODEL: When a user's session is initiated (from the User Domain), the identification and authentication requirements are based on the level of trust needed to transit the network (Transport Domain) and access the desired data or services (Data Domain). The trust level required depends on the sensitivity of the data or services being requested. The trust level is derived from the required authentication process and the connectivity path. As outlined below, the domain trust levels indicate whether additional authentication is required before access to the data domain is permitted. Trust Levels are defined as:

- Level 0 Absolute trust (e.g., biometrics, face-to-face, personal knowledge of identity, etc.).
- Level 1 Assured trust (e.g., token authentication with PIN, unique user ID and password from a pre-certified location).
- Level 2 Conditional Trust (e.g., unique user ID and password).
- Level 3 Semi-public trust (e.g., uses only a password, no userids).
- Level 4 Public trust (e.g., no security).

D. Access Controls - Session Management and Transport

3.11 FIREWALLS - SECURE ROUTING: Anytime sensitive or proprietary information is routed on a network, the issue of network partitioning becomes extremely important. In all cases, there will be some information which should not be transmitted outside a certain area, or to any node which is considered vulnerable or accessible by an unauthorized user. In order to enforce network partitioning, "firewalls" ***MUST*** be constructed to control routing of traffic.

a. Protocol Filtering: A common tool used in partitioning networks is the use of protocol filtering. This involves the administration of "filters" at a gateway, router, or firewall, which control what traffic may pass through the network. The firewall looks at certain fields within the packet header, and triggers the filter, which decides to permit or deny the packet based on an access control list. Some TCP/IP services are inherently insecure and ***MUST*** be blocked at the initial point of entering the SWBT network. Refer to Appendix 2 for a listing of the services

that will be prohibited by default from locations outside the SWBT network. Current systems, or applications/programs that utilize the prohibited services with an origination point outside the SWBT network, ***MUST*** be re-engineered by December 31, 1995.

b. Application Gateways: Application gateways consist of a host which is dedicated to process and route traffic for a given application, e.g., mail, FTP and telnet. Application gateways have proven to be very effective in a TCP/IP network although they generally require more "work" than protocol filtering.

3.12 CENTRALIZED SECURITY SERVER: To standardize security features and protection, application and system security ***SHOULD*** be used in conjunction with transport security mechanisms wherever possible. SWBT is rapidly moving toward having all user requests to access or transit the SWBT DCN being authenticated by a centralized security server. This model facilitates SWBT requiring a one-time password (using the security server) for all external access to SWBT systems/DCNs.

3.13 TERMINAL TIMEOUTS: Terminals or other input devices ***MUST NOT*** be left unattended while they may be used for system access. After a reasonable period of inactivity (e.g., 15 minutes), the screen ***SHOULD*** be blanked and either the keyboard locked (i.e., the user's password is used to regain access) or the terminal ***SHOULD*** be disconnected. Upon completion of each work session, a terminal which is other than a trust level 0 ***MUST*** be properly logged off and all transactions cleared. The DCN or connected system ***MUST*** automatically end a session when a device logs off, is timed out, or there is an apparent disconnect.

3.14 DIAL-UP ACCESS: Installation of dial-up devices ***MUST*** comply with the provisions of Operating Practice No. 118 (OP118). Dial-up access to trust level 0/1 data or transport domains (i.e., a SWBT DCN) ***MUST*** be protected with a biometrics or token based (e.g., one-time password) authentication system. In special cases, dial-up devices ***MAY*** be used if access is strictly controlled for each session (e.g., the secure password is immediately changed at the end of the session).

3.15 SOCIAL ENGINEERING: Social engineering is a request, usually by phone, for a userid and/or password by an unknown person who impersonates an authorized user. Employees ***MUST NOT*** give access information to unknown persons. Telephone requests for dial-up access to SWBT systems or DCNs ***MUST NOT*** be granted without positive authentication of the requestor.

3.16 SECURE TRANSMISSION OF DATA: Sensitive or private information (e.g., authentication data) ***MUST*** be encrypted when transmitted over a SWBT DCN. Encryption is the responsibility of the application or security server.

E. Identification Controls - Userids

3.17 AUTHORIZING DCN USERS: All authorized DCN users ***MUST*** be uniquely identified to support individual accountability and auditing. A userid (in MicroLinkII, a Network User Id or NUI) distinguishes a given user from all other users recognized by the DCN. Within SWBT, the unique userid is assigned by the Standard User-Id Tracking System (SUITS) system and ***MUST*** be used on all SWBT systems.

a. Userid Standard Formats - A standard (SUITS) userid has a maximum length of seven (7) characters. In SWBT systems, there are three standard formats that are based on the classification of the user.

b. SWBT Employee Userid - Initially derived from the SWBT payroll system (2 initials and the final four numbers of the SSN with an alphabetic used in position 6 to resolve conflicts).

c. System/Application Userid - A unique identification code is required when a system accesses other systems. While the userid ***SHOULD NOT*** exceed seven characters, System Administration ***MAY*** select a desired userid, as long as it is unique between the involved systems, which simplifies the identification of the system (e.g., a COSMOS system/machine in St. Louis might be assigned mec001 where me = Mechanized, c = St. Louis' division code, and 001 = system number).

d. Non-SWBT Userid - A user from Southwestern Bell Corporation (SBC) or an SBC National Subsidiary, a contract employee, vendor, customer, client, or a user on a non-SWBT network who requires regular access to SWBT information resources. These users ***MUST*** be sponsored by a SWBT employee and have a unique userid permanently assigned and maintained by system administration or the departmental coordinator. To emphasize user accountability, a format similar to the SWBT employee format is strongly recommended.

3.18 SYSTEM USERID TRACKING SYSTEM (SUITS): The SUITS system operates in conjunction with SWBT's PHONE application to ensure the unique assignment of userids from SWBT personnel records. SUITS uses

employee/agent SSNs to track all permanent SWBT userids and their administrative information. The SUITS System Administrator (a member of CSAG) may be contacted through the CORINET help desk (314 235-3412).

3.19 USERID AUTHORIZATION: The organization that grants access and issues userids ***MUST*** develop and document a process to approve all new users. An appropriate paper or E-mail record ***MUST*** be maintained by the Security Administrator of when and to whom access was granted. The original form ***MUST*** be signed by the user or appropriate manager to confirm that the new user understands his/her responsibilities. Appendix 5 from OP113 or an equivalent document can be used for this process.

3.20 USERID SHARING: To ensure personal accountability, userids ***MUST NOT*** be shared.

3.21 USERID VALIDATION: Each month, all userids ***MUST*** be re-verified that they are associated with an active SWBT employee, Company agent, system, or customer (a mechanical comparison against SUITS is strongly recommended). Invalid userids ***SHOULD*** be immediately deactivated and recent usage investigated. Non-SWBT userids ***MUST*** be re-authenticated by the associated SWBT sponsor every 90 days. The list of userids on a system/DCN must be provided to SUITS for the semi-annual verification. SUITS will then provide a composite report to SWBT managers/sponsors of valid users and the systems to which they have access.

3.22 VENDOR DEFAULTS: Security Administrators ***MUST*** strictly control any vendor access to SWBT systems and ***NEVER*** retain a vendor supplied userid/password.

F. Authentication Controls - Passwords, Token-Cards

3.23 AUTHENTICATION FUNCTION: Verifies the identity of a user who is trying to access a system. In SWBT, authentication is achieved by using a password or a token card which generates a one-time password. A password or the one-time password generated by a token card is PERSONAL and PRIVATE information which ***SHOULD*** never be shared (including maintaining a supervisory list); each user is responsible for maintaining and protecting his/her passwords. Unfortunately, passwords are increasingly vulnerable to attacks that compromise their confidentiality. Consequently, it is desirable that networks evolve to support more secure mechanisms for authentication, e.g., cryptographically based third party servers, smart-card tokens, etc.

3.24 COMPLETE AUTHENTICATION: The security system ***MUST*** complete the entire authentication process before permitting any activity, even if the userid itself is invalid. Error feedback on which part of the authentication information is incorrect ***MUST NOT*** be given to the user.

3.25 PASSWORD FORMAT: Passwords ***MUST*** be 6-8 characters in length; a non-dictionary word; non-null; contain at least one number and one alphabetic/special character (if the system permits special characters). Numerics and special characters can be placed at the beginning or end as long as a numeric or special character is embedded somewhere else within the password. The password ***MUST NOT*** be the same as or a reverse of the userid or the system name. The password field of any userid in the password file ***MUST NOT*** be blank (all userids ***SHOULD*** have some entry in the password field, e.g., VOID, EXPIRED, *, x, etc.).

3.26 INITIAL PASSWORD: When a password is initially assigned or it is necessary to administratively change it, a change-on-first-use procedure ***MUST*** be implemented which requires the user to immediately change it to a personal password upon the first access.

3.27 PASSWORD DISPLAY: DCN systems ***MUST NOT*** display or print passwords during the login process. Internal password files ***MUST*** have restricted access, the password field ***MUST*** be encrypted or a shadowing scheme employed.

3.28 PASSWORD EXPIRATION/AGING: DCN systems which do not have password history functionality, ***MUST*** assign passwords with both minimum and maximum aging requirements and automatically expire within 31 days for general users. Systems with password history functionality ***MUST*** comply with the maximum aging and expiration policies. Certain users (e.g., system administrators, user administration, etc.), due to their authority level and the critical nature of their activities, ***MAY*** require a shorter period (e.g., 7 days or less). Systems ***SHOULD*** notify users at expiration time and allow on-line updating of the user's password.

3.29 PASSWORD REUSE: When available,the security software ***SHOULD*** minimize a given user's reuse of his/her password. For most users, a reasonable limit is no reuse for 6 changes/months.

3.30 TOKEN-CARDS: If token-cards are used for access, the token-card and its security information (e.g., seed, associated userid, etc.) ***MUST*** be tracked, issued and activated by the centralized Token Card Administrator (see CSAG, Section 1.14, for contact information). Usage of token-cards

SHOULD be included as part of the userid verification process (see Section 3.21). OP113, Appendix 2, should be used to request token card registration.

G. Authorization Controls - Controlling Access to Resources

3.31 CONNECTING TO NON-SWBT DCNS/SYSTEMS: Connections to non-SWBT DCNs/systems are permitted only for approved Company business. The Company firewall ***MUST*** be the only entry point to SWBT DCNs for non-SWBT IP addresses (e.g., dial-in connections, access from the Internet, access by clients, etc.).

3.32 TCP/IP ADDRESS CONTROLS: A TCP/IP based DCN uses IP address information to route internal traffic. However, filtering by IP address ***SHOULD NOT*** be used as a replacement for identifying the individual user. Userid authentication ***SHOULD*** be the primary basis for granting permission to use resources. IP filtering ***MAY*** be used to control application-to-application traffic within a secure DCN. Within the DCN, traffic should be limited to internal IP addresses wherever possible (e.g., LAN segments would not permit an IP address from outside the company to enter the Company WAN).

3.33 DCN ACCESS RULES: The number of DCN privileged users with access to system/security files ***MUST*** be minimized and activity with these files strictly controlled and monitored. Vendors, other non-SWBT, or non-operations personnel ***SHOULD*** have their access rights limited to single sessions (e.g., change userid password after each session, keep token card under the control of SWBT personnel, etc.) unless there is a clear business need for recurring access.

3.34 DCN ACCESS ADMINISTRATION: The network ***MUST*** provide the ability to grant access rights to DCN applications to a single user or group of users as well as deny access rights to a single user or a group of users. DCN default access rights ***MUST*** be to the creator of a resource or an appropriate administrator.

3.35 ACCESS CONTROL LISTS: Individual systems and applications are expected to maintain their own resource access control methodology. The DCN's primary function is to provide connectivity between users, agents, and applications. Where possible, the DCN will support a centralized identification/authentication service to properly validate users who request resources from an access control list.

H. Monitoring and Auditing Functions

3.36 AUDIT LOG: The network ***MUST*** generate a security log that contains information sufficient for after-the-fact investigation of loss or impropriety. The userid associated with any request or activity ***MUST*** be maintained and passed on to any other connected environments so that the initiating user identity can be traceable for the lifetime of the request. The network security log ***MUST*** be protected from unauthorized access or destruction and retained for at least 90 days.

a. The audit log ***MUST*** record at least the following:

- Invalid user authentication attempts
- Unauthorized attempts to access resources
- Changes to a users security profiles and attributes
- Changes to the access rights of resources
- Changes to the network security configuration (e.g., routing to a security server)
- Modification of network software
- Replay attacks.

b. For each event, the audit log record ***MUST*** include at least:

- Date and time of the event
- User identification
- Associated terminal, port, network address, or device
- Type of event
- Names of resources accessed
- Success or failure of the event.

3.37 SECURITY EVENTS (REPORTING): Suspected or actual intrusion events (e.g., attempting or actually gaining unauthorized access to a system or its resources) ***MUST*** be reported to the departmental organization responsible for computer security. They in turn, ***MUST*** report to Asset Protection at 314 331-2434. If unsure about reporting an event, contact an ISF representative or Asset Protection for advice.

3.38 BANNER (ACCESS WARNING): To notify users of the ownership of network resources and deter unauthorized access events, an access warning message ***MUST*** be displayed at the first point of entry until a subsequent transaction is executed. Legally, users requesting access ***MUST*** be notified of the Company which owns the resources. OP113 has

three acceptable versions of the warning (a full length one and two shorter versions). The standard full-length OP113 message text is:

> ***"This is a Southwestern Bell Telephone Company system, restricted to Company official business and subject to being monitored at any time. Anyone using this system expressly consents to such monitoring and to any evidence of unauthorized access, use, or modification being used for criminal prosecution."***

3.39 LOGINS (INVALID ATTEMPTS): A session ***MUST*** be ended if an unreasonable number (maximum three) of logon attempts (i.e., invalid userid/password combinations) are made.

3.40 DISPLAY LAST LOGIN: The DCN security service must display the last successful login date/time and the number of invalid login attempts since last login upon successful login.

3.41 INACTIVE USERIDS: Valid userids which have no activity for 90 days ***MUST*** be reviewed for deactivation or deletion (for non-SWBT userids, this is done by the SWBT sponsor). Weekly, the CSAG group sends to all ISF members and selected Security Administrators a list of newly inactive SWBT employees (resignations, retirees, transfers, etc.). System/Security Administrators ***MUST*** delete these employees from the system password/shadow file.

3.42 VALIDATING PASSWORD FILES: Procedures ***MUST*** be implemented to periodically check the password file for the existence of null passwords or the potential of an individual password being cracked. Any "cracker" type programs ***MUST NOT*** be kept online in either source or compiled form and ***MUST*** be access restricted to system administration.

I. Reviewing System Security

3.43 ANNUAL REVIEW REQUIREMENT: In accordance with OP113, an annual review of each system's security features and procedures ***MUST*** be completed by the System and Security Administrators. This review ***MUST*** be documented and retained for the life of the system. Appendix 1, Annual Security Review - Data Communication Networks ***SHOULD*** be used for this process.

3.44 TRUST LEVEL VERIFICATION: All connections between SWBT systems and SWBT or public transport domains ***MUST*** be regularly verified to ensure

that appropriate trust levels are maintained. This ***SHOULD*** be done during the annual security review, when new connectivity is added, or whenever trust levels change. More detailed information about trust levels, data domains, etc., may be found in OP113, starting at Section 4.3.

3.45 EXCEPTION REPORTING AND DOCUMENTATION: Deviations uncovered during the review process ***MUST*** be documented on the review form and resolved as soon as practicable. If the deviation cannot be corrected by consultation with a subject matter expert, or the compliance item is considered unnecessary, unreasonable, or not possible, a risk acceptance ***MUST*** be prepared. It should include a cost benefit analysis, a plan to correct the deficiency, and interim procedures to provide appropriate protection. This report ***MUST*** be approved by the associated departmental Director, forwarded to the ISF Chairperson for review, and retained for the life of the system. Send exception reports to the ISF Chairperson, see CSAG in Section 1.14.

4. CONTINGENCY PLANNING

A. Information Services

4.01 IS CONTINGENCY PLANNING: Information Services' Computer Security Administration Group (CSAG) is also responsible for policies and procedures on IS Contingency Planning. Questions on these issues should be directed to the CSAG Contingency Planning specialist at 314 235-5813 or to the CSAG in accordance with SW910 Section 1.14.

4.02 EXECUTIVE RECOVERY MANUAL (ERM): The Information Services' Computer Security Administration Group (CSAG) maintains an ERM to identify key operations and personnel in the event of a disaster in a data center. This manual is updated quarterly with current contact information and issued to each Information Services Director as well as the data center site coordinators.

4.03 EMERGENCY OPERATIONS CENTER (EOC): The EOC is a command center for Information Services in the event of a disaster. The Computer Security Administration Group maintains the EOC documentation, coordinates EOC testing, and the management of the center during a disaster. Questions on the EOC should be directed to the ECC coordinator at 314 235-0237 or to the CSAG (see Section 1.14).

4.04 APPLICATION RECOVERY MANUAL (ARM): As with other applications, the DCN ***MUST*** have a documented disaster recovery process. This

document ***SHOULD*** be maintained by the DCN System Administrator. Instructions for mid-range systems are contained in SW 007-590-909 (SW909), Documenting Minicomputer Disaster Recovery Plans, microcomputers in SW911, and mainframes in SW 007-590-906 (SW906), Disaster Recovery/Computer Facility Contingency Planning.

4.05 SITE RECOVERY MANUAL (SRM): Each System Administrator ***MUST*** have documented, the local procedures in the event of a disaster. This supplements the information supplied in the ARM. Special considerations such as off-premise information, routing information, etc. ***SHOULD*** be documented in the SRM.

B. User Departments

4.06 RECOVERIES: User departments ***SHOULD*** work closely with the DCN operations as well as applications support groups to understand the requirements of recovering their applications. Some issues of concern are:

- How do user groups perform their jobs while the DCN is being recovered?
- How is missing daily activity recovered (e.g., toll calls which had been processed but the master files were destroyed in the disaster, etc.) ?

4.07 PROCESSING (LONG-TERM OUTAGE): User groups ***SHOULD*** develop procedures for performing their jobs in the event of the DCN or their application(s) not being available for an extended period (i.e., 30 days or more). User department management is responsible for verifying compliance within each work group. Project managers and leaders ***SHOULD*** review options such as:

- Is the application data available from some other source?
- Could work be done from periodic snapshots of application data (e.g., a paper printout, a copy of the master file loaded on another system, etc.)?