APPLICATION SECURITY CHECKLIST

Instructions:

1. PURPOSE OF A REVIEW: OP113, Protection of Electronic Information, requires timely reviews of the security controls involved in all phases of a system's development and processing. A single review ***SHOULD*** cover all programs or applications which process as an "entity" (e.g., one for DOPAC, another for TIRKS, etc.). To comply with OP113, Sections 3.04 and 3.07 of SW912 require a review of internal security controls whenever a significant change is made to the program or the operating environment.

   Each review should be used to assess the overall level of information protection provided by the software and supplemented by the operating environment, hardware, and relevant operating procedures. A proper review provides direction on how to maintain and/or increase the level of information protection in a system.

2. PERSONNEL INVOLVED: The review ***MUST*** be performed by the SWBT or contract employees who perform the Project Manager and Project Leader functions. These functions/jobs are defined in Section 3 of SW912.

3. ADMINISTRATIVE ITEMS: The following items ***MUST*** be included: review date, application/system name, names of reviewing personnel, items reviewed and their status: "Yes" (in compliance, either the application or operating environment), "N/A" (not applicable), or "No" (a deviation which requires an exception report). An explanation ***MUST*** be attached to describe each "N/A" or "No" answer. The completed review ***MUST*** be retained with program documentation for future reference and audit reviews.

4. ITEMS TO BE REVIEWED: The following pages include areas from SW912 to be covered in a review. Each Project Leader ***MUST*** document any additional areas of concern that are specific to his program and/or operating environment (the expression "AOE" on the checklist stands for "application or operating environment"). When a given operating environment satisfies a control, the environment's code (see listing below for code assignments) has been placed in the column labeled OPER. ENVIR "Yes." This question does ***NOT*** need to be re-answered or an exception filed ***UNLESS*** the operating environment standards are ***NOT*** being followed. Partial complies are indicated with a small code letter (i.e., "d" in place of "D" for a DEC/VAX system) and ***MAY*** need to be answered. All other questions ***MUST*** be answered and any exceptions documented as required.

   - **"D" (DEC/VAX):** #4 (timeout) and #5 (disconnection) comply if HITMAN is used; #11 (standard userids) complies if conversion is complete.

PROPRIETARY
Not for use or disclosure outside of Southwestern Bell
Telephone Company except under written agreement

APPLICATION SECURITY CHECKLIST

- **"R" (MVS/RACF):** #8 (simultaneous use) and #24 (displaying logon info) ***CANNOT*** comply for IMS applications.

- **"T" (TANDEM):** #5 (disconnection) complies only on the test system.

- **"U" (UNISYS):** #17 (password display) and #24 (displaying logon info) comply ***ONLY*** for the UNIX side of UNISYS (with UNISYS demand logon procedures, the userid and password are entered together and logon attempts are not displayed).

- **"V" (VM):** #1 (warning message) complies under VTAM access.

- **"X" (UNIX):** #1 (warning message) and #19 (password complexity) comply for System 5 release 3 or later; #13 (privileged userid monitoring) complies if SU to root commands are sent to the system console/hard copy; #22 (audit log protected) complies if #21 (audit log used) is answered yes.

5. EXCEPTIONS UNCOVERED: Section 4.10 of SW912 describes the exception process for areas not in compliance with SW912 and OP113. Exceptions ***MUST*** be fully documented and resolved as soon as practicable. If a requirement is considered unnecessary, unreasonable, or not possible, it ***MUST*** be reviewed with the department's GHQ ISF member or the CSAG Group (see Section 1.11). If this review does not resolve the issues, a written exception ***MUST*** be submitted to the Program Director for Information Security through the ISF as described in Section 3.04.

6. TRACKING EXCEPTIONS: The exception report ***MUST*** be approved by the system's departmental division manager and retained for the life of the system. It must include a cost benefit analysis, a plan to correct the deficiency, and interim procedures to provide appropriate protection.

7. QUESTIONS ON REVIEW PROCESS: Specific questions on hardware or software should be referred to the appropriate SWBT specialists. General questions on policy or procedures may be referred to an Interdepartmental Security Forum (ISF) departmental representative or the ISF Chairperson (see SW912, Section 3.04).

APPLICATION SECURITY CHECKLIST

Review Date: ____________ Application/System: ______________________

Project Mgr: ____________________ Project Leader: ______________________
Phone: ____________________ Phone: ______________________

(Attach an explanation for each answer of "N/A" or "No")

SW912 SECT	SECURITY AREA/REQUIREMENT	OPER. ENVIR "Yes"	Yes N/A No
	AREA: Access Control - General Requirements		
4.12	1. Is a SWBT standard warning message displayed ***BEFORE*** logon?	D R T U v x	
4.15	2. Are userids used to grant only the minimum privileges to do the user's job?		
4.16	3. Do system defaults limit file/data access to the creator of the data?	R U V	
4.18	4. Are inactive terminals automatically password locked or logged off (timeout)?	R U V	
4.19	5. If the user ends the session without logging off, does the AOE terminate the session?	d R t U V	
	AREA: Identification - Userids		
4.20	6. Are all users (systems/applications and individuals) required to be assigned a unique userid (no programmed group userids)?		
4.20	7. Is information to identify the user associated with each userid?		
4.21	8. Do all userids use a SWBT standard format (SWBT employee, non-SWBT employee, or system/application)?	d R T U V	
4.22	9. Are privileged/system userids strictly monitored and controlled?	R U T V x	
4.23	10. Does the application or operating environment (AOE) maintain the identity of each user?	D R T U V X	
4.24	11. Can the AOE provide a list of valid userids and their allowed actions and/or permissions?	D R T U V X	

APPLICATION SECURITY CHECKLIST

Review Date: __________ Application/System: ________________

SW912 SECT	SECURITY AREA/REQUIREMENT	OPER. ENVIR "Yes"	Yes N/A No
AREA: Authentication - Passwords & Tokens			
4.26	12. Is the entire authentication process completed before error notification?		
4.27	13. Is a complete authentication required before allowing password changes?		
4.27	14. Is a change-on-first-use password required for initial or administratively changed passwords?		
4.28a	15. Is each userid required to use an individual password or token authenticator?	D R T U V X	
4.28b	16. Is the clear-text display of passwords suppressed?	D R T u V X	
4.28c	17. Is the internal password file or passwords encrypted and access restricted?	D R T U V X	
4.28d	18. Does the password comply with OP113 (6-8 characters; not blank or the userid; and at least one character, other than the first or last one, a number/special character)?	D R U V x	
4.29	19. Are passwords aged, the user notified of expiration, and allowed on-line updating?	D R U V	
4.30	20. Is a password restricted from reuse for some period (e.g., 6 months)?		
AREA: Authorization - Access to Restrictions			
4.32	21. Are all users required to identify themselves *BEFORE* any action can take place?	D R T U V X	
4.33	22. Is there a mechanism to associate userids with similar privileges?		
4.34	23. Are system access control data files/tables protected from unauthorized access?	D R T U V X	

APPLICATION SECURITY CHECKLIST

Review Date: __________ Application/System: ______________

SW912 SECT	SECURITY AREA/REQUIREMENT	OPER. ENVIR "Yes"	Yes N/A No
4.35	24. Are non-privileged users kept from unauthorized access of the operating environment?	D R T U V X	
4.36	25. Is simultaneous use of a userid restricted (e.g., prevented or the users are notified of use in real-time)?	r U V	
4.37	26. If program "backdoors" are used, are they fully documented and coordinated?		
4.38	27. Is there a mechanism to remove or deactivate inactive userids?		
	AREA: Monitoring & Audit Mechanisms		
4.40	28. Is an audit log used and data maintained for a reasonable period (e.g., 6 months)?	R U V	
4.41	29. Is the audit log protected from unauthorized access/modifications?	D R V x	
4.42	30. Is a session terminated after 3 invalid logon attempts?	R U V	
4.43	31. Is the user's last valid logon time and any invalid logon attempts displayed after successful logon?	D r u V	
	AREA: Application Development Procedures		
5.02	32. Is separation-of-duties or an equivalent procedure used to ensure application integrity?		
5.03	33. When the sensitivity or vulnerability of the data changes is a new risk analysis performed?		
5.05	34. Is sensitive information protected when transmitted over untrusted networks or connections?		
5.07	35. Are appropriate error detection and integrity controls programmed into the application?		

PROPRIETARY
Not for use or disclosure outside of Southwestern Bell
Telephone Company except under written agreement

APPLICATION SECURITY CHECKLIST

Review Date: __________ Application/System: ________________

SW912 SECT	SECURITY AREA/REQUIREMENT	OPER. ENVIR "Yes"	Yes N/A No
5.10	36. Is all software authorized, appropriately licensed and acquired?		
5.11	37. Is developing, copying, or using software or other mechanisms to bypass security clearly prohibited?		
5.12	38. Is a formal test and analysis of security controls documented?		
5.14 5.15	39. Were all security features fully tested and errors corrected?		
5.16	40. Are development and live operations systems kept physically separate or equivalent alternative procedures used?		
5.17	41. Are changes to program code authorized and documented appropriately?		
5.18	42. Are application security contacts identified and contact procedures documented?		
5.19	43. Are there procedures for receiving and installing software releases?		
5.20	44. Are emergency program changes approved and documented?		
5.23	45. Is there a formal security administrator's guide with complete instructions?	R U	
5.24	46. Are all system operator procedures for security features documented?	R U	
5.25	47. Are required security procedures documented for clients/end-users?		
	AREA: Continuity of Service		
6.01	48. Are non-privileged users prevented from deliberately or accidentally making the system unavailable to other users?	D R T V X	
6.02	49. Is there a documented back-up procedure for data and programs?		

APPLICATION SECURITY CHECKLIST

Review Date: __________ Application/System: ________________

SW912 SECT	SECURITY AREA/REQUIREMENT	OPER. ENVIR "Yes"	Yes N/A No
6.03	50. Is a master copy of software protected from unauthorized modification and destruction?		
6.04	51. Is there a documented recovery procedure?		

PROPRIETARY
Not for use or disclosure outside of Southwestern Bell Telephone Company except under written agreement

APPLICATION SECURITY CHECKLIST

Review Date: __________ Application/System: ________________

(This page is intentionally left blank)