INTERNAL AUDIT PROGRAM DATA CENTER REVIEW

DATA CENTER REVIEW PROGRAM

Our objectives are to ensure:

- The physical security and access control measures are adequate to prevent unauthorized access to computer center areas.
- The environmental controls are adequate to minimize hardware / software losses from fire or flood.

PROCEDURE	RESPONSE	W/P REF.
I PRELIMINARY PROCEDURES:		
A. Obtain a current list of personnel, (including positions), responsible for maintaining the programs, backing up the system/data files, and using the computer center systems.		
B. Obtain a schedule or document an overview of the Information Systems Including hardware resources, software, support/design staff, and users) in the Computer Center • Determine the overall criticalness of each major system identified • On dial-in lines does the security system include callback features or some other means of control to ensure authorized access?		
C. Review the previous audit report and note items to be followed up during the current audit. Determine if management has taken appropriate and timely action to address the deficiencies noted in the audit report.		
D. Review any examination reports received since the last audit. Determine if management has taken appropriate and timely action to address the deficiencies noted.		
II PHYSICAL SECURITY		
A. Determine the geographical location of the Data Center and evaluate the overall risks.		
B. Identify any additional hardware storage locations (e.g. Servers, Gateway's, Bridges, Routers, Multiplexors etc) and evaluate their physical security. (e.g. Telecommunication Rooms, Electrical Switchgear Rooms).	*(what other locations connect to this facility?)*	
C. Assure that there are written procedures in effect, which prevent unauthorized persons from gaining access to computer facilities.	*(obtain copies of procedure manuals)*	
D. Assess the building's security program and		

PROCEDURE	**RESPONSE**	**W/P REF.**
describe the equipment and/or other measures the data facility uses to provide protection. (e.g. CCTV)		
E. Determine that the computer room is equipped with locks to limit access, and those access devices are properly assigned and accounted for. (Access devices may be keys, magnetic cards, or combinations.)		
F. If keys or magnetic cards are used, verify that they are accounted for by an inventory control and recovered if the assigned individual leaves the Company's employment or moves to a job that does not warrant access to the computer facility.		
G. If combination locks are used, verify that they are changed on a regular basis to ensure that the usefulness of a combination known to a former employee would be short-lived.		
H. Determine the basis on which individuals are given keys, cards, or combinations to the computer room. Access should be on a need-to-enter basis only. (For example, the president does not have a need to enter, but the computer operator does. Need is not a function of rank, but of job responsibilities.)	*(obtain procedure manual)*	
I. Through observation, determine that doors to the computer room are kept locked at all times.		
J. Determine that a log of access to the computer room is maintained. The log should contain at least the signatures of individuals who are not regularly on duty in the computer room.		
K. Determine that when anyone who is not regularly assigned to the computer room enters the secure area, that individual has to sign an entry log.		
L. Verify that a list of persons authorized to be in the computer room is posted in plain sight, and that individuals not on the list are required to be accompanied by individuals who are so authorized. (No one should be allowed in the computer room, including check-processing areas, without authorization or sponsorship and without the presence of an official who is authorized to grant access to the computer room).		
M. Determine that service technicians are identified by official documents from their employers until they are well known and recognized by the staff of the computer		

INTERNAL AUDIT PROGRAM DATA CENTER REVIEW

PROCEDURE	RESPONSE	W/P REF.
room.		
N. Determine how any unauthorized hardware components added to the network would be detected.		
III FIRE PROTECTION SYSTEMS	(describe Fire Protection Systems)	
A. Ascertain if the computer room has an adequate and safe fire-suppression system with associated detectors (heat, smoke, and water) and whether other necessary environmental controls are in use.		
B. Ensure fire-suppression equipment would effectively extinguish fires without harm to equipment and documents in the computer room.		
C. Confirm that the area immediately surrounding the Data Center is free from combustible materials. (Note: Physical Security over Data Centers must extend to the areas immediately surrounding the Data Center. The reason for this is attributed to the fact that most fires start outside the Data Center and then spread in.)		
D. Determine that the computer is protected by an Uninterruptible Power Source (UPS) to ensure smooth transition of operations in the event of power failure.		
E. The computer room should be kept clean at all times.		
F. Determine if fire protection systems are regularly tested.		
IV ENVIRONMENTAL CONTROLS		
A. The environmental equipment and controls should be adequate to protect the computer hardware from damage. Use the following areas as a guideline in determining adequacy.		
B. Ventilation and air conditioning should be adequate to maintain appropriate temperature level specified by the manufacturer.		
C. Recording thermometers and humidity indicators should be located so the readings can be obtained easily. A trained person should monitor these instruments on a routine basis.		
D. The hardware should automatically shut down to protect itself from damage if unacceptable temperatures reached.		
E. The computer equipment should be subject		

INTERNAL AUDIT PROGRAM DATA CENTER REVIEW

PROCEDURE	RESPONSE	W/P REF.
to periodic maintenance, cleaning and inspection and a record kept of such.		
F. The computer room ceiling should be adequately constructed to prevent water from entering the computer room.		
G. Overhead water steam and pipes should be avoided.		
H. Adequate drainage should be provided.		
I. Are the floors raised?		
J. Independent air conditioning system with backup power supply should be installed.		
V EMERGENCY PROCEDURES		
A. Determine if the posted emergency procedures address: • Instructions for shutting off utilities. • Instructions for powering down equipment. • Instructions for activating/deactivating fire suppression equipment. • Personnel evacuation. • Security valuable assets.		
Determine if emergency procedures are conspicuously posted throughout the organization.		
Determine whether employees are familiar with their duties and responsibilities in an emergency situation and whether an adequate employee-training program has been implemented.		
Determine the notification procedures to: Management and Clients/Customers		
Confirm that backup copies of data are maintained in off-site.		
VI CONCLUSIONS:		