Agency **Audit Program - Physical Security**		Initials	Date
	Prepared By		
	Reviewed By		
	W / P Ref		
	Page **1** of **1**		

Procedures	Initials	Date	Reference/Comments
OBJECTIVE - To document the review of the physical security over computer operations. This program is used to itemize the procedures utilized to allow the auditor to assess the control environment..			
1. Utilize the Physical Security Internal Control Structure Questionnaire to gain an understanding of the control procedures. In completing the ICSQ, include the following: **a. results from interviews that further describe the control procedures** **b. documentation that illustrates the current conditions pertaining to the control procedures.**			
2. Summarize control policies and procedures (initial assessment) identified in developing an understanding of the physical security controls. Include the most significant control policies and procedures that might be tested to provide evidence of their operating effectiveness.			
3. If it is determined to be effective and efficient, design and perform tests which will provide evidence of the operating effectiveness for significant control policies and procedures determined in #2 above.			

Procedures	Initials	Date	Reference/Comments
4. Based upon the above procedures, include any weaknesses on a point disposition sheet. Weaknesses should be discussed with management and finding sheets should be written for reportable conditions.			
5. Include the audit results in an overall memo. Consider the effect of the results, combined with the results of any other ICSQ performed, on the overall control environment.			

		Initials	Date
Agency **Internal Control Structure Questionnaire** **Physical Security** Updated: 10/95	Prepared By		
	Reviewed By		
	W/P Ref		
	Page **1** of **6**		

INSTRUCTIONS NEEDED FOR COMPLETION OF THE QUESTIONNAIRE:

1. The responses to the questions in the ICSQ will be used in gaining and documenting an understanding of the EDP General control structure.

2. Assess the level of control risk for each accounting system or control procedure listed on the ICSQ using the following measures of risk:

   0 - Low Risk
   1 - Moderate Risk
   2 - Slightly Less Than Maximum Risk
   3 - Maximum risk

   Document your justification for the level of risk assessed in the space provided.

3. Cross-reference to flowcharts, narratives, memorandums, etc. that support the control policies or procedures, when applicable.

4. The ICSQ will be maintained in the permanent file rather than the current workpapers. See new permanent file maintenance instructions for further information.

5. The ICSQ can have items added or deleted depending on the particular needs of the current audit.

For clarification or assistance, contact the EDP Audit Specialist Team Coordinator

Policy/Question	N/A	Yes	No	W/P - Remarks
CONTROL POLICY #1 - The responsibility for physical security is assigned.				
1. Has responsibility been assigned for the following? **a. access to the computer building** **b. access to computer room** **c. access to libraries** **d. fire prevention** **e. prevention from other hazards**				
2. Are there written policies for security over the data processing facility?				
3. Are the responsibilities for physical security documented in job descriptions?				

Circle the level of Control Risk assessed for this Control Procedure:

0 - Low Risk
1 - Moderate Risk
2 - Slightly Less Than Maximum Risk
3 - Maximum risk

RISK ASSESSMENT JUSTIFICATION:

Policy/Question	N/A	Yes	No	W/P - Remarks
CONTROL POLICY #2 - Physical access to the computer room, libraries, and building is restricted to authorized personnel.				
1. Is access to the computer room limited to operators and other employees whose job duties require physical access to the computer equipment?				
2. Are methods used to prevent unauthorized access to the computer room, such as the following? **a. wearing badges by all data processing personnel** **b. requiring visitors to wear badges** **c. requiring keys, passcodes, or magnetic cards for entrance** **d. the presence of a receptionist or guard** **e. use of a sign-in log** **f. collecting keys and badges and/or changing codes when employees terminate** **g. remote cameras** **h. motion detectors**				
3. Is physical access to the libraries restricted to the librarian or person responsible for the data?				
4. Is there security for the building housing the computer facility such as the following? **a. fences** **b. exterior lighting** **c. remote cameras** **d. building guards** e. police surveillance f. sign-in log for after hours g. building locks				

Circle the level of Control Risk assessed for this Control Procedure:

0 - Low Risk
1 - Moderate Risk
2 - Slightly Less Than Maximum Risk
3 - Maximum risk

RISK ASSESSMENT JUSTIFICATION:

Policy/Question	N/A	Yes	No	W/P - Remarks
CONTROL POLICY #3 - Data processing resources are protected from fire, water, and other potential hazards.				
1. Are the following techniques used to detect and extinguish a fire? **a. smoke or heat detectors, including detectors under the floor and above the ceilings** **b. periodic testing of smoke or heat detectors** **c. an automatic extinguisher system which is periodically inspected or hand-held extinguishers that are easily accessible, regularly inspected, and identified as to their type and use**				
2. Is there protection against water damage in the computer room and libraries, such as the following? **a. the computer room being located in an area that is not subject to flooding** **b. inspection and securing of water pipes in the ceiling or walls to prevent damage to hardware** **c. a watertight floor** **d. sealed windows to prevent water from coming in** **e. water detectors under the floor** **f. shut-off valves for water pipes**				
3. Is the climate of the computer room and libraries controlled for the following? **a. humidity** **b. accidental and/or intentional shut down of the air conditioning unit**				

Policy/Question	N/A	Yes	No	W/P - Remarks
4. Does security training for data processing employees include the following? **a. what to do when an alarm sounds** **b. evacuation from the building** **c. notifying the appropriate authorities (security officers, police, fire department) of the emergency** **d. performing emergency shutdown of the computer equipment** **e. assisting with the removal of equipment and records, if necessary** **f. training in fire prevention and use of fire extinguishers** **g. challenging of unauthorized personnel in the computer room**				
5. Do the libraries and computer room meet the following criteria? **a. solid walls that are fire resistant and extend to the solid or true ceilings** **b. solid doors that are fire resistant** **c. fire resistant floors, furniture, drapes, and other furnishings**				
6. Are the computer room activities controlled to prevent fire by the following? **a. prohibiting smoking in the computer room** **b. storing cleaning rags, cleaning fluids, paper stock, and trash outside the computer room.**				
7. Is there adequate protection against power outages and power surges by the following? **a. monitoring and recording voltage** **b. an alternate power source** **c. emergency lighting**				
8. Are there means for reporting an emergency, such as the following? **a. the presence of an alarm pull box** **b. an alarm that sounds in the computer room** **c. an alarm that sounds in a remote location**				

Policy/Question	N/A	Yes	No	W/P - Remarks
9. Are there plans for evacuation in case of an emergency, such as the following? **a. escape routes that are posted and kept open** **b. an emergency evacuation plan** **c. periodic evacuation drills**				

Circle the level of Control Risk assessed for this Control Procedure:

0 - Low Risk
1 - Moderate Risk
2 - Slightly Less Than Maximum Risk
3 - Maximum risk

RISK ASSESSMENT JUSTIFICATION:

Physical Security Control Procedure Information

CONTROL POLICY #1 - The responsibility for physical security is assigned.

Written procedures and responsibilities for physical security should be documented. Responsibility should encompass access to the computer building, the computer room, and software documentation libraries. In addition, responsibility for prevention from fire and other hazards should be assigned. The job descriptions for the Physical Security Administrator should be written to ensure the responsibilities for physical security is documented.

The auditor should interview the person responsible for Physical Security. The job description should be reviewed to ensure responsibilities for Physical Security have been assigned.

CONTROL POLICY #2 - Physical access to the computer room, libraries, and building is restricted to authorized persons.

Access to the computer room should be limited to operators and other employees whose job duties require physical access to the computer equipment, the computer room, and documentation. The methods used to prevent unauthorized access to the computer room may include such as the wearing badges by all data processing personnel, requiring visitors to wear badges, requiring keys, passcodes, or magnetic cards for entrance, the presence of a receptionist or guard, use of a sign-in log, remote cameras, and motion detectors.

The auditor should observe and document the physical access capabilities to the computer room, libraries, and building. Weaknesses noted should be discussed with management.

CONTROL POLICY #3 - Data processing resources are protected from fire, water, and other potential hazards.

Physical Security Measures - Smoke or heat detectors, including detectors under the floor and above the ceilings, should be used to detect and extinguish a fire. There should be periodic testing of smoke or heat detectors, and inspection of automatic extinguisher systems. Any hand-held extinguishers should be easily accessible, regularly inspected, and identified as to their type and use.

The libraries and computer room should have solid walls that are fire resistant and extend from floor to solid or true ceilings. There should be solid doors, furniture, drapes, and other furnishings that are fire resistant. In addition, smoking in the computer room should be

prohibited, and the storing cleaning rags, cleaning fluids, paper stock, and trash should be outside the computer room.

Auxiliary Power Sources - Adequate protection against power outages and power surge should exist and an alternate power source with emergency lighting should be installed. There should be visible means for reporting an emergency, such as the presence of an alarm pull box, an alarm that sounds in the computer room and in a remote location.

Water Protection - Protective measures on against water damage in the computer room and libraries, such as the computer room being located in an area that is not subject to flooding, and the water pipes are in the ceiling or walls to prevent damage to hardware should exist. In addition, climate control for the computer room and libraries that monitor the humidity levels and prevent the accidental and/or intentionally shut down of the air-conditioning unit should be installed.

Physical Security Training - Security training for data processing employees include what to do when an alarm sounds, evacuation from the building, and the notification of the appropriate authorities (security officers, a police, fire department) of the emergency. Procedures for the emergency shutdown of the computer should be written. In addition, the removal of equipment and records, training in fire prevention, and use of fire extinguishers should be documented. Means for physical evacuation should include escape routes that are posted and kept open. There should be a documented emergency evacuation plan with periodic evacuation drills.

The auditor should observe and document the environmental and protective aspects over data processing resources. Physical Security training test results (fire drills) should be obtained and evaluated. Weaknesses noted should be discussed with management.