**November**

**Audit Report**

**South Bay Latino Research Center**

**Purpose**

In this audit, the South Bay Latino Research Centre (SBLC)'s information systems will be checked for security issues. It will also be used to check that the changes made after the last audit were implemented.

**Outcome**

The outcome of this audit will be recommendations for the research center on how to better improve the security system by finding loopholes if there are any and providing solutions.

**Scope**

The scope of the audit is to check whether the SBLRC's information security policies, processes, and measures work, are sufficient, and are followed. We will check the network, systems, and endpoints for security controls, settings, and holes. Examine encryption techniques, access controls, and data processing procedures for sensitive data. We will be evaluating the controls for access management, authorization, and user authentication. We would also evaluate security practices of third-party vendors and their impact on SBLRC's security posture.

**Audit Procedure**

**Arrival**: The audit team will arrive at the South Bay Latino Center and contact Mr. Jose Limon (The IS/IT lead), for an access code and authorization to proceed. Audit team will then walk into the facility using the access code to gauge staff reactions.

**Introduction**: Once audit team is satisfied with the entry exercise, they will introduce themselves to Mr. Limon and his team

**Audit Meeting**: Once introduced, the audit team will work with Mr. Limon and members of the staff, as requested, to complete the attached audit plan documentation. Items may be added to the audit plan as necessary and as agreed between the audit team and Mr. Limon These items will be documented using the blank lines in the audit plan.

**Audit Hot Wash**: Once the audit team has completed the attached Audit Plan document the audit team will inform Mr. Limon that the audit is complete and will then conduct a post audit meeting him. The purpose of this meeting will be for the audit team to convey initial findings and for the audit team and Mr. Limon to generate and agree on any needed action plan.

**Mariam Adegbindin Audit Complete (time/date):**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | | **Audit Plan:**  **Items and Observations**  **Auditor: Date:** | | | |
| **Item #** | **Description** | | **Expected Findings/pass criteria** | **Observations** | **Pass (Yes/No)** |
| 1 | Check the Policy for managing IoT devices | | Review and validate existence of policy for managing and maintaining IoT devices |  |  |
| 2 | Check MFA Implementation | | Review MFA configurations for critical systems and user accounts |  |  |
| 3 | Check the contingency plan | | Verify the update and testing of the SBRLC contingency plan |  |  |
| 4 | Check that personnel’s have been properly trained | | Confirm that training sessions for SBRLC personnel and Mr. Limon have been conducted |  |  |
| 5 | Check updates & submission of security plan | | Review the plan for currency, accuracy and alignment with industry standards |  |  |
| 6 | Check the progress of IS/IT initiatives in collaboration with SDSURF and SDSU | | Assess communication channels and information sharing mechanisms between entities |  |  |
| 7 | Check physical security | | Review access controls and surveillance  Check if the walls are all the way up to ascertain if access can be gained through the ceiling |  |  |
| 8 | Check data security | | Review data handling and encryption to ensure confidentiality of sensitive information |  |  |
| 9 | Verify vulnerability scans using shield’s up are done, evaluated, and retained | | Monthly scans are being performed and evaluated |  |  |
| 10 | Check for malware control process | | No malware found |  |  |
|  |  | |  |  |  |
| 11 | Check for process to ensure updates are being incorporated on organizational computers | | Computers are up to date with auto updates on |  |  |
| 12 | Check for proper handling of secure waste | | Shred boxes and other processes in place |  |  |
| 13 | Check the server room | | Confirming that the temperature is cool and not warm |  |  |
| 14 | Shred box | | Confirm that there is a shred box for documents to ensure proper disposal of sensitive information |  |  |
| 15 | File Cabinets | | File cabinets to store documents to ensure that they are not just placed anywhere that is especially accessible to unauthorized personnel. |  |  |
| 16 | Looking at the Network segmentation, firewalls, intrusion detection and prevention systems | | There should be divided network architecture to separate sensitive information and important systems. |  |  |
| 17 | Assessing security practices of vendors and third-party partners. | | Using due diligence to check the security policies of third parties and following the terms of contracts on security. |  |  |
|  |  | |  |  |  |
|  |  | |  |  |  |
|  |  | |  |  |  |
|  |  | |  |  |  |
|  |  | |  |  |  |
|  |  | |  |  |  |
|  |  | |  |  |  |
|  |  | |  |  |  |
|  |  | |  |  |  |
|  |  | |  |  |  |
|  |  | |  |  |  |
|  |  | |  |  |  |
|  |  | |  |  |  |