Fougnigue Sefon
CIDM 6341
Audit plan report

Audit Plan for SBLRC

Purpose

The purpose of this audit is to systematically review and assess the information security and operational practices within the San Diego Biomedical Research Center (SBLRC). The focus will be on ensuring compliance with established policies, identifying areas of improvement, and providing recommendations for enhancing the overall security posture and efficiency of research operations.

Outcome

The outcome of this audit will be recommendations for strengthening the security and operational posture of SBLRC.

Scope

The scope of this audit plan is Password management, Staff training procedures, IoT policy, Contingency planning, Database & Server security, Offboarding & Onboarding process, and physical security.

Audit Procedure

Arrival: The auditor Fougnigue Sefon will arrive at the San Diego Biomedical Research Center and contact Jose Limon, the IT lead for an access code to proceed. The auditor will then walk into the facility using the code to gauge staff reactions.

Introduction: Once Fougnigue Sefon is satisfied with the entry exercise they will introduce themselves to John McGill, the director of the research center.

Audit Meeting: Once introduced, the auditor/audit team will work with (put contact name here) and any 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 auditor/audit team and (put contact name here). These items will be documented using the blank lines in the audit plan.

Audit Hot Wash: Once the auditor has completed the attached Audit Plan document he will inform Jose Limon that the audit is complete and will then conduct a post audit meeting with John McGill. The purpose of this meeting will be for Fougnigue Sefon to convey initial findings and agree on any needed action plan/further information needed/potential recommendations/etc..

Audit Commenced (time/date): **Audit Complete (time/date):**

Auditor:

Fougnigue Sefon
501-340-322

	Audit Plan: **Items and Observations** **Auditor:**			**Date:**
Item #	**Description**	**Expected Findings/pass criteria**	**Observations**	**Pass (Yes/No)**
1	Check password process	Should be compliant with the SDSU process		
2	SBLRC Staff training	Employees have received proper training after high turnover due to COVID		
3	IOT Policy	An IOT Policy has been included in the security plan		
4	Check for contingency plan	Updated contingency plan that reflects current personnel, location and practices		
5	Check for multifactor authentication	MultiFactor Authentication has been implemented for section 7.5		
6	Verify vulnerability scans using shield's up are done, evaluated, and retained	Monthly scans are still being performed and evaluated		

7	Check for contingency plan	Contingency plan has been tested		
8	Check for database security	Database has been fully and securely migrated to MongoDB		
9	Check for servers	Servers have been securely migrated to the SDSU cloud		
10	Check for data retention policies	compliance with data retention policies for both physical and electronic records		
11	Check for monitoring system	Monitoring systems have been implemented to ensure timely detection of security incidents		
12	Check for data privacy and security	compliance with data disposal and destruction policies to prevent unauthorized access		
13	Check for data privacy and security	compliance with regulatory requirements related to research data handling and storage		
14	Check for data privacy and security	backup procedures are in place and regularly tested for reliability		
15	Check for physical security	effectiveness of the research center regarding protection of individuals		
16	Check for physical security	In compliance with physical security measures for data storage and equipment		
17	Check for data classification	compliance with data classification policies to ensure appropriate		

		handling of different types of research data		
18	Check for	compliance with export control regulations for research projects with international collaborators		
19	Check for implementation of secure communication channels for sensitive research discussions and collaborations	Implemented		
20	Check for data privacy and security	controls are in place to protect research center information from insider threats and unauthorized access by employees.		
21	Check for Offboarding process	departing employees have their access revoked across all systems		
22	Check for offboarding process	standardized checklist or procedure in place to guide the offboarding process,		