June 24, 2018

**Audit Plan for Pacific College of Oriental Medicine**

**Purpose**

The purpose of this audit is to conduct a review of the PACIFIC COLLEGE Information Systems Security Plan (ISSP), server configurations, and physical security to determine compliance with applicable regulations and standards.

**Outcome**

The outcome of this audit will be documented in the attached table of Audit Items and Observations, to include the pass criteria for each item audited, the observed findings, and determination of compliance scored as either pass or fail.

**Scope**

This audit plan is limited to the PACIFIC COLLEGE ISSP, server security, and physical security. The audit will not provide a comprehensive review of each of these categories but will provide a focused review of the topics deemed to be most critical, as agreed upon by the audit team and the PACIFIC COLLEGE Information Systems Security Officer (ISSO).

The following regulations will be used to determine compliance:

* FIPS 199 Standards for Security Categorization of Federal Information and Information Systems
* NIST SP 800-53 Rev. 4 Security and Privacy Controls for Federal Information Systems
* and Organizations
* NIST SP 800-171 Protecting Controlled Unclassified Information in NonFederal Information Systems and Organizations
* NIST Cybersecurity Framework Version 1.1
* Gramm-Leach-Bliley Act (GLBA)

**Audit Procedure**

**Arrival**: The audit team will arrive at PACIFIC COLLEGE and contact the ISSO for authorization to proceed. The audit team will then walk into the facility using the authorized access method to gauge staff reactions and commence the audit. The audit team may attempt to social engineer staff into allowing the audit team access to the server room or other secure areas of the building.

**Introduction**: Once the audit team is satisfied with the entry exercise, they will announce their identity and have the ISSO verify them.

**Audit Meeting**: Once the audit team identity has been verified by the ISSO, the audit team will work with the staff members identified by the ISSO to complete the attached audit list of items to be audited. Items may be added to the audit plan as necessary and as agreed upon by the audit team and the ISSO.

**Audit Hot Wash**: Once the audit team has completed the attached list of Audit Items and Observations, the audit team will announce that the audit is complete and will then conduct a post audit meeting with the ISSO. The purpose of this meeting will be for the audit team to convey initial findings and for the audit team and ISSO to generate and agree on any needed action plan, further information needed, potential recommendations, etc.

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

**Audit Team: Information Systems Security Officer:**

Christian Larsen Alexander Diaz

Harshal Sanap

Iliya Shuster

Jeremy Silverstein

Alessandro Vomero

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Audit Plan:** ISSP, Server Security, Physical Security **Date:** June 27, 2018  **Auditors**: Christian Larsen, Harshal Sanap, Iliya Shuster, Jeremy Silverstein, Alessandro Vomero  **Items and Observations** | | | | |
| **Item #** | **Description** | **Expected Findings/pass criteria** | **Observations** | **Pass (Yes/No)** |
| 1 | ISSP: identification of applicable standards | The ISSP cites applicable standards (e.g, NIST SP 800-53 Rev. 4, SP 800-171, and the GLBA.) |  |  |
| 2 | ISSP: current ISSP approved | The ISSP has been approved by organization-defined personnel (ISSO at minimum). NIST SP 800-53 Rev. 4 PL-2 SECURITY PLANNING POLICY AND PROCEDURES |  |  |
| 3 | ISSP: updated when applicable standards change | The Organization has a documented process for regular review and update of the ISSP. NIST SP 800-53 Rev. 4 PL-2 SECURITY PLANNING POLICY AND PROCEDURES |  |  |
| 4 | ISSP: management of user accounts | The organization manages user accounts per NIST SP 800-53 Rev. 4 AC-2 ACCOUNT MANAGEMENT. |  |  |
| 5 | ISSP: compliance with external media use policy | The organization adheres to the policy outlined in the ISSP for use of flash drives on workstations. NIST SP 800-53 Rev. 4 MP-7 MEDIA USE. |  |  |
| 6 | Server Security: vulnerability management program | The organization follows a documented vulnerability management program to identify and resolve vulnerabilities on servers in a timely manner per NIST SP 800-53 Rev. 4 RA-5 VULNERABILITY SCANNING. |  |  |
| 7 | Server Security: password complexity and age requirements | Passwords comply with NIST SP 800-53 Rev. 4 IA-5(1) PASSWORD-BASED AUTHENTICATION. |  |  |
| 8 | Server Security: physical inventory | Inventory of devices (servers and workstations) is accurate and up to date. NIST SP 800-53 Rev. 4 CM-8, PM-5 |  |  |
| 9 | Server Security: protection of data-at-rest | Sensitive data is encrypted while being stored on AWS servers. NIST SP 800-53 Rev. 4 MP-8, SC-12, SC-28 |  |  |
| 10 | Server Security: configuration control and management | Servers are configured according to company approved baselines. All changes are documented in CM program. NIST SP 800-53 Rev. 4 CM-1 CONFIGURATION MANAGEMENT |  |  |
| 11 | Physical Security: server room security log | The organization monitors access to the server room through the use of a security log (written or electronic). NIST SP 800-53 Rev. 4 PE-3 PHYSICAL ACCESS CONTROL |  |  |
| 12 | Physical Security: fire protection controls in place for the server room | The organization protects the server room with necessary fire protection. NIST SP 800-53 Rev. 4 PE-13 |  |  |
| 13 | Physical Security: water damage protection for designated rooms | The organization has controls in place to prevent flooding in the server room and other designated rooms. NIST SP 800-53 Rev. 4 PE-15 |  |  |
| 14 | Physical Security: emergency power is available for critical systems | The organization provides short-term UPS capability to allow for server shut-down. NIST SP 800-53 Rev. 4 PE-11 EMERGENCY POWER |  |  |
| 15 | Physical Security: server room temperature and humidity control | The organization maintains temperature and humidity levels within the facility where information systems reside. NIST SP 800-53 Rev. 4 PE-14 TEMPERATURE AND HUMIDITY CONTROLS |  |  |
| 16 |  |  |  |  |
| 17 |  |  |  |  |
| 18 |  |  |  |  |
| 19 |  |  |  |  |
| 20 |  |  |  |  |
| 21 |  |  |  |  |
| 22 |  |  |  |  |
| 23 |  |  |  |  |
| 24 |  |  |  |  |
| 25 |  |  |  |  |