**Audit Plan for The Office of Career & Professional Development (OPCD)**

**at West Texas A&M University**

**Purpose**

The purpose of this audit is to assess the operations and security measures of the Office of Career and Professional Development at West Texas A&M University. Additionally, we will review the physical security and security processes related to career services.

**Outcome**

The outcome of this audit will be recommendations for improving the efficiency and security of career services.

**Scope**

The scope of the audit is to check whether the OPCD information security policies, processes, and measures work, are sufficient, and are followed. We will check the network, systems, and endpoints for security controls, and settings. 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.

**Audit Procedure**

**Arrival**: The auditor will arrive at the Office of Career and Professional Development (OPCD) and contact Kat Kane the director of the OPCD, for authorization to proceed. Auditor will then walk through the office using authorization to gauge staff reactions.

**Introduction**: Once auditor is satisfied with the entry exercise, they will introduce themselves to the staff members.

**Audit Meeting**: Once introduced, the auditor Mariam Adegbindin and any members of the staff, as requested will complete the attached audit plan documentation. Items may be added to the audit plan as necessary and as agreed between the auditor and Kat. 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 the auditor will inform Kat that the audit is complete and will then conduct a post audit meeting with Kat. The purpose of this meeting will be for the auditor to convey initial findings and for the auditor and Kat to generate and agree on any needed action plan.

**Audit Commenced (time/date): 4/23/2024 9:00am, Audit Complete (time/date): 4/23/2024 5:00pm**

**Auditor: Mariam Adegbindin**

**(Put contact name here): Kat Kane**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | | **Audit Plan:**  **Items and Observations**  **Auditor: Date:** | | | |
| **Item #** | **Description** | | **Expected Findings/pass criteria** | **Observations** | **Pass (Yes/No)** |
| 1 | Review of Organizational Structure and Policies | | Clear organizational structure defined with documented policies and procedures for career services. | Organizational chart and policy documents are readily available and clearly outline roles and procedures. | Yes |
| 2 | Review of Policy for managing IoT devices | | Existence of policy for managing and maintaining IoT devices | A policy document outlining procedures for managing and maintaining IoT devices is available. | Yes |
| 3 | Confirmation of Staff Training | | Completion of training sessions for personnel on cybersecurity measures | Staff members have taken cybersecurity training courses online provided by the school. | Yes |
| 4 | Assessment of Collaboration with IT Entities | | Communication channels and information sharing with IT entities | Effective communication channels are established between the OPCD and IT entities. | Yes |
| 5 | Examination of Physical Security | | Access controls, surveillance, and physical barriers | Access to the office is not restricted, the doors are left opened when a staff steps out and so can lead to unauthorized entry | No |
| 6 | Ensuring Update Incorporation on Organizational Computers | | Compliance with update procedures and utilization of auto updates | Organizational computers are configured to receive automatic updates. | Yes |
| 7 | Confirmation of Proper Handling of Secure Waste | | Secure disposal methods for sensitive information | Secure shredding bins are available and used for proper disposal of sensitive documents. | Yes |
| 8 | Verification of Shred Box Existence | | Presence of shred box for proper disposal of sensitive documents | There is no designated shred box located in the office for disposal of sensitive documents. | No |
| 9 | Secure Storage of Documents | | Use of file cabinets for secure document storage | Documents are stored in locked file cabinets to prevent unauthorized access. | Yes |
| 10 | Assessment of Multi-Factor Authentication (MFA) | | Configuration and implementation of MFA for critical systems and user accounts | Multi-factor authentication is enabled for critical systems and user accounts requiring heightened security. | Yes |
| 11 | Evaluation of Compliance with Regulatory Standards | | Compliance with relevant legal and regulatory standards, such as those related to student privacy (FERPA) and employment laws. | The office is compliant with FERPA and other relevant regulatory standards governing student privacy and employment laws. | Yes |
| 12 | Check for Access Control on Personal Files | | Only computer owner can access all files | Access to personal files is restricted to authorized users only. | Yes |
| 13 | Check for Other Digital Devices | | No other devices | Printer and several iPads | Yes |
| 14 | If Additional Devices Discovered Check for the above on them | | Passwords, backups, access control exist | There are no passwords for the iPad | No |
| 15 | Check Password Strength. | | Should be strong: no dictionary word | Passwords are complex and do not contain dictionary words. | Yes |
| 16 | Check Data Security | | Review data handling and encryption to ensure confidentiality of sensitive information | Data handling procedures ensure confidentiality, and encryption protocols are in place for sensitive information. | Yes |
| 17 | Evaluation of Contingency Plan | | Update and testing of the contingency plan | The contingency plan is regularly updated and tested to ensure effectiveness in case of emergencies. | Yes |
| 18 | Review of Security Plan Updates | | Currency, accuracy, and alignment with industry standards of security plan | The security plan is updated regularly, accurate, and aligned with industry best practices. | Yes |
| 19 | Assessment of Digital Devices Room Conditions | | Adequate temperature control and security measures in the server room | The device room is properly temperature controlled but there is no restricted access in place as someone from another department can go in to take an office supply | No |
| 20 | Assessment of Vendor and Third-Party Security Practices | | Due diligence in checking security policies and contractual terms regarding security with vendors and third-party partners | Due diligence is performed to ensure vendors and third-party partners adhere to security policies and contractual terms. | Yes |
| 21 | Check for surge protection on power supply | | Surge protection present | No surge protectors present | No |
| 22 | Computer is kept in a location with controlled access | | Access is limited to those with a need | Computers are in secure areas accessible only to authorized personnel. | Yes |
| 23 | Check for Ransomware response/recovery plan | | Existence and effectiveness of response/recovery plan | A response and recovery plan for ransomware attacks is covered by the IT department of the school | Yes |
|  |  | |  |  |  |
|  |  | |  |  |  |
|  |  | |  |  |  |
|  |  | |  |  |  |
|  |  | |  |  |  |
|  |  | |  |  |  |
|  |  | |  |  |  |
|  |  | |  |  |  |