Audit Plan for Law Firm

Purpose

The purpose of this audit is to check the Law Firm's office for any vulnerabilities in securing any sensitive data stored at the Law Firm.

Outcome

The outcome of this audit will be recommendations for the office manager of the Law Firm.

Scope

The scope of the audit is the Internet connection, computer, data processes and physical security of the Law Firm's office.

Audit Procedure

Arrival: The auditor will arrive at the office of the Law Firm and contact the office manager, Xxxx Xxxxxx for an access code/access/authorization to proceed. Auditor will then walk into the facility using the code/access/authorization to gauge staff reactions.

Introduction: Once auditor is satisfied with the entry exercise, the auditor will introduce herself to Ms. Xxxxxx.

Audit Meeting: Once introduced, the auditor will work with Ms. Xxxxxx 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 and Ms. Xxxxxx. 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 Ms. Xxxxxx that the audit is complete and will then conduct a post audit meeting with Ms. Xxxxxx. The purpose of this meeting will be for the auditor to convey initial findings and for the auditor and Ms. Xxxxxx to generate and agree on any needed action plan/further information needed/potential recommendations/etc..

Audit Commenced (time/date):1100, 4/21/2023 **Audit Complete (time/date):**

Auditor:

Xxxx Xxxxxx**:**

	Audit Plan: Items and Observations Auditor: Penelope Tello			Date: 4/21/23
Item #	**Description**	**Expected Findings/pass criteria**	**Observations**	**Pass (Yes/No)**
1	Check how far the office's wireless network can be found away from the office	Wireless network cannot be found past the parking lot of the office		
2	Check that the router is password protected	Router is password protected		
3	Check employees' knowledge of phishing emails and websites	Employees know about phishing emails and websites		
4	Check if any ports are open on the computers at the office, using ShieldsUP	Ports should all be in stealth or at least closed		
5	Check if any emails or phone numbers used by the office have been disclosed, using HaveIBeenPwned	Emails and phone numbers should show as not having been disclosed during any data breaches		
6	Check strength of passwords used at the office	Passwords should be at least 10 characters long, have at least one uppercase letter, one lowercase letter, one number, and one system-acceptable special character		
7	Check that computers in the office have antivirus software	All computers in the office should have active antivirus software		
8	Check that the computers in the office are not missing any updates	All computers in the office are up to date and have auto updates on		
9	Check that the office has some type of firewall technology in place	Office has firewall technology in place		
10	Check if anyone that does not work in the office can	No one that does not currently work inside the office should be		

	access sensitive data stored in the office	able to access sensitive data		
11	Check for at least one back up for data storage	Back up for data storage exists on a physical device or on the cloud		
12	Check for any procedures in place for limiting access to any sensitive data when an employee no longer works at the office	Past employees should not have any access to sensitive data		
13	Check for any procedures in place to limit employees' access to sensitive data when they are away from the office	Employees should not have access to sensitive data when they are away from the office		
14	Check for any procedures in place for disposing of sensitive data and network devices, like shredding	Documents with sensitive data that need to be disposed of should be shredded and any network devices that need to be disposed of should be properly done so		
15	Check that the office is in a safe area	Office should be in a safe area		
16	Check the office for any protection mechanisms in place like a fence, gate, alarms, and/or locks	Office should at least have locks and alarms		
17	Check that there is only one point of entry into the office	Office should only have one point of entry		
18	Check that hard copies of sensitive data are stored in secure locations that can be locked like a lockable filing cabinet	Hard copies of sensitive data should be stored in secure locations		
19	Check that the office has a working security system	Office should at least have a security system in place to protect windows, doors, and point(s) of entry		
20	Check that the office has a secure room for servers/network devices	Office has a secure room for servers/network devices		

21	Check that the office has backup power supplies	Office has backup power supplies		
22	Check that the office uses surge protectors	Office should use surge protectors and change them at least once a year		
23	Check if there is software installed to track down the computers, if stolen	Computers should have software installed that can be used to track the computers in case of theft		
24	Check for a fire detection system in the office	Office has a fire detection system		
25	Check for a fire extinguisher in the office	Office has a fire extinguisher		
26	Check that the environment for areas with digital devices is kept clean, cool, and smoke-free and has good air flow	These areas are kept clean, cool, and smoke-free and have good air flow		
27	Check if the office has a custodial staff	If the office has a custodial staff, the custodial staff should not have unsupervised access to digital devices and/or sensitive data		