Audit Plan for EZ Fencing

Purpose

The purpose of this audit is to check the security of the company computer and access control for EZ Fencing as well as check the physical security processes of the company.

Outcome

The outcome of this audit will be recommendations for the owner of EZ Fencing.

Scope

The scope of the audit is the Internet connection, computer, and data processes.

Audit Procedure

Arrival: The auditor/audit team will arrive at the company and contact the owner, Angel Caballero, for an access code/access/authorization to proceed. Auditor/audit team will then walk into the facility using the code/access/authorization to gauge staff reactions.

Introduction: Once auditor/audit team is satisfied with the entry exercise they will introduce themselves to Angel Caballero.

Audit Meeting: Once introduced, the auditor/audit team will work with Angel 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 Angel. These items will be documented using the blank lines in the audit plan.

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

Audit Commenced (time/date): 9:30am - 11/20/24 Audit Complete (time/date): 10:30am - 11/20/24

Auditor: Sera Hill

Angel Caballero:

	Audit Plan: Items and Observations Auditor: Sera Hill Date: 11/7/2024			
Item #	**Description**	**Expected Findings/pass criteria**	**Observations**	**Pass (Yes/No)**
1	See if internet connection can be accessed by unauthorized users	Router is password protected, and are encrypted	Router is protected by a password and the network is hidden but not encrypted	No
2	Check for password protection for router	Must have proper credentials to gain access to the router	Only owner has login credentials, must add devices to network himself	Yes
3	Check for physical to router is secure	Router is kept in secure, locked location, away from the public	Router is in locked home office	Yes
4	Ensure proper environment for router (good airflow, secure location)	Airflow and location are fine	Router is in adequate location	Yes
5	Verify only authorized devices are connected to the network	Only company devices are connected	Only approved devices are on network	Yes
6	Check ports on computer	Should be closed or in stealth	All ports are in stealth	Yes
7	Check if firewall and malware protections are active	Firewall and malware protection are active	No firewall or malware protection	No
8	Check if computer is up to date	Computer is up to date and auto updates are active	Not up to date, no auto updates enabled	No
9	Check password strength	Ensure it follows NIST guidelines (password length, no common words)	Strong password, follows NIST guidelines	Yes
10	Check if computer password has been compromised	Computer password has not been found in any data breaches	Password has not been found in any breaches	Yes
11	Check for access control for personal files on computer	Personal documents aren’t accessible by low-level users	There are user restriction in place	Yes
12	Check proper user permissions exist for all users on computer	Only owner has admin rights to computer, lower level users can’t access everything	User restrictions are in place, no passwords are saved to keychain	Yes

13	Ensure confidential customer information is stored securely	Confidential files are password protected	No customer information is stored on computer, kept in physical cabinet on paper	Yes
14	Check if user activity is monitored	User activity is checked for employees	Owner regularly checks applications and ensures proper users are logged in	Yes
15	Check physical access to computer is secure	Computer is kept in secure, locked location, away from the public	Computer is kept in locked home office	Yes
16	Check for security camera backups	Camera footage is backed up	No backups, footage is kept for 30 days and saved off if an incident occurs	No
17	Ensure access control exists for security camera footage	Only owner can access security camera footage	Only owner is able to access security footage feed	Yes
18	Check for computer backup	Backups exist	No backups	No
19	Check if backups are tested	Backups are checked periodically	No backups	No
20	Ask about a security plan	Security plan exists	No plan	No
21	Ask about incident response plan	Incident response plan exists	Rough plan exists	Yes
22	Check if access control is reviewed periodically	Periodic review of user permissions exist	Review occurs at least once a week	Yes
23	Check if company email has been compromised	Email has not been found in data breaches	Not found in data breach	Yes