**Audit Plan for One Stop Remodeling and Roofing**

**Purpose**

The purpose of this audit is to evaluate computer systems, data management, and physical security of One Stop Remodeling and Roofing, a small construction company. The main goal is to prioritize and identify potential risks and ensure proper operations are being followed that suit the business appropriately.

**Outcome**

The outcome of this audit will be recommendations for One Stop Remodeling and Roofing.

**Scope**

The scope of the audit is the Internet connection, computer, and data processes. Customer data is a particularly sensitive subject in this business, establishing secure data handling is imperative.

**Audit Procedure**

**Arrival**: The auditor/audit team will arrive at 1506 E Central Ave, Amarillo, TX and contact the foreman, Tanner Jones, for access and authorization to proceed. Auditor/audit team will then walk into the place of business using the access/authorization to gauge daily operations.

**Introduction**: Once auditor/audit team is satisfied with the entry exercise they meet with owner, Joseph Skinner.

**Audit Meeting**: Once established, the auditor/audit team will work with Tanner Jones and any members also available, 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 Joseph Skinner. 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 Joseph Skinner that the audit is complete and will then conduct a post audit meeting with Joseph Skinner and Tanner Jones. The purpose of this meeting will be for the auditor/audit team to convey initial findings and for the auditor/audit team to generate and agree on any needed action plan/further information needed/potential recommendations/etc.

**Audit Commenced (time/date): 2:00 PM on 11/15/2024**

**Audit Complete (time/date): 3:47 PM on 11/15/2024**

**Auditor: Aubrey Skinner**

**(Put contact name here):**

**Joseph Skinner, owner**

**Tanner Jones, foreman**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | | **Audit Plan:**  **Items and Observations**  **Auditor: Aubrey Skinner Date: 11/15/2024** | | | |
| **Item #** | **Description** | | **Expected Findings/pass criteria** | **Observations** | **Pass (Yes/No)** |
| 1 | Physical Security of Premises | | Windows are locked, door has a lock, are both criteria met when room unattended | Room where computers and files are located had locked windows, no locked door but was shut. Unlocked window found in bathroom. | No |
| 2 | Access Control | | Does the computer have a password | Computer has a passcode. Passcode also found to be unique and no pwnage found on Have I Been Pwned. | Yes |
| 3 | Systems Update | | Regular updates for all software to mitigate vulnerabilities | Software updates found to be behind on both computer (Dell) and work cell phone (iPhone). | No |
| 4 | Printer Security | | Printed documents are monitored and documents promptly retrieved | No documents in printer tray, no visible documents laying around printer. | Yes |
| 5 | Document Disposal | | Are confidential customer documents disposed of properly (i.e. shredding) | Paper shredder is present on site, no visible documents laying around in the open. | Yes |
| 6 | Remote Work Security | | When away from the premises, is there secure remote access | Only access is when physically present at the site of the computers and other hardware. | No |
| 7 | Internet Connection | | Stable internet connection with appropriate security settings | Internet connection tested with Speedcheck, download speed at 36.41 Mbps and upload speed at 37.06 Mbps. This represents an internet connection not suitable for a company. Security settings were in place. | No |
| 8 | Malware | | Active, up-to-date antivirus software, malware scans are conducted | Malware protection found and is up to date, working properly. | Yes |
| 9 | Employee Cybersecurity Awareness | | Staff trained on cybersecurity manners as to protect customer data | Customer communication found to be through Facebook Messenger on staff cell phones. Unsecured form of communication for customer data. | No |
| 10 | Data Organization | | Data is organized and in appropriate folders/files | Desk drawers containing physical paperwork are behind a lock and organized appropriately. | Yes |
| 11 | Incident Response | | The business has a clear plan/ existence of incident response in the event of employee injury, cyber-attacks, etc. | No existence of any sort of emergency plan for any events. | No |
| 12 | Data Backup | | Regular data backups to either cloud or external | Cloud backups are turned on and up to date for both company cell phone and computers. | Yes |
| 13 | Physical Security | | Desk containing customer information is locked or securely guarded | Desk drawers with private customer data are behind a lock and were locked during audit. | Yes |
| 14 | Mobile Device Security | | Mobile devices used for customer communication are secured with PINs or facial recognition | All phones used for customer communication are equipped with both PIN numbers and facial recognition. | Yes |
| 15 | Password Management | | Use of strong passwords, regular password changes. Password recovery in place | Password recovery in place for major sites used to conduct business. 2 email address and/or phone number and email address in place for recovery. Passwords not found pwned on Have I Been Pwned. | Yes |
| 16 | Social Engineering Awareness | | Employees trained to recognize phishing and report it | Staff employee was quizzed on phishing using OpenDNS website. Employee passed with 12/14. | Yes |
| 17 | Digital Signature | | Digital signatures used for contracts/ documentation requires authentication | Digital signatures found on Adobe Acrobat do not require authentication. | No |
| 18 | Security of Entry Points | | Exterior doors are equipped with functioning locks and locked when business is not within operating hours | Exterior doors equipped with working locks, owner states they always remain locked outside of business hours. | Yes |
| 19 | Risk Assessment | | Business conducts risk assessments to identify potential vulnerabilities | No history of a risk assessment being performed. | No |
| 20 | Bookkeeping | | Financial records are kept and maintained regularly and reviewed | Bookkeeping is up to date and accurate. Finances are regularly reviewed. | Yes |