**Audit Plan for Palace Coffee**

**Purpose**

The purpose of this cybersecurity audit is to assess the current state of Palace Coffee’s network and computer systems security and identify any vulnerabilities or potential security threats.

**Outcome**

The ultimate goal is to provide Palace Coffee with recommendations to improve their cybersecurity posture and mitigate potential security risks.

**Scope**

The audit aims to evaluate Palace Coffee’s current cybersecurity practices, including network security, password policies, data backup and recovery, employee cybersecurity awareness, PCI DSS compliance, and incident response plan.

**Audit Procedure**

**Arrival**: The auditor (myself) will arrive at the Palace Coffee shop and make contact with the appropriate personnel to gain access to the premises.

**Introduction**: I will introduce myself and explain the purpose of the audit to the appropriate personnel. I should also request any necessary access codes or authorizations to begin the audit process. While on the premises, I will conduct myself professionally and unobtrusively to avoid causing alarm or disruption.

**Audit Meeting**: Once introduced, I will work with the owner(s) (Patrick and Krystal Burns) 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 (put contact name here). These items will be documented using the blank lines in the audit plan.

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

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

**Auditor: Jordan Unfred**

**Patrick and Krystal Burns:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | | **Audit Plan:**  **Items and Observations**  **Auditor: Jordan Unfred Date: 4/18/2023** | | | |
| **Item #** | **Description** | | **Expected Findings/pass criteria** | **Observations** | **Pass (Yes/No)** |
| 1 | Identify all hardware, expected and unexpected | | POS system, router, or any other hardware is expected and accounted for |  |  |
| 2 | Identify software used on hardware | | No unexpected/unsafe software |  |  |
| 3 | Document make and model of each expected inventory device | | No unexpected hardware found on network |  |  |
| 4 | Check password age and complexity on devices | | Constantly renewed with no dictionary words |  |  |
| 5 | Review computer files for possible malware | | No malware found |  |  |
| 6 | Check that computer is up to date on latest security and patches | | Computer is up to date |  |  |
| 7 | Check current malware protection | | Security is operational with zero threats |  |  |
| 8 | Check for backup | | Backup exists |  |  |
| 9 | Check power supply and surge protection on each hardware device | | Power supplies and surge protectors are not overloaded and clean |  |  |
| 10 | Check router in secure location | | Router is inaccessible to unpermitted individuals |  |  |
| 11 | Check router air flow | | No dust on vents, clean cable management |  |  |
| 12 | Check network for vulnerabilities (Nessus, Qualys, ShieldsUp) | | No vulnerabilities found |  |  |
| 13 | Check for MFA | | MFA in use |  |  |
| 14 | Check firewall and make sure it is up-to-date with the latest patches | | Firewall patches are up to date |  |  |
| 15 | Check firewall that it’s configured to block unnecessary traffic | | Firewall only allows necessary traffic for its operations |  |  |
| 16 | Check PCI DSS complies with encryption | | Cardholder data encrypted |  |  |
| 17 | Incident response plan utilization | | A response plan is ready for any cybersecurity incidents with defined roles and responsibilities, communication procedures |  |  |
| 18 | Check for any assets requiring inventory | | No other devices |  |  |
| 19 | If any additional devices discovered, perform Item # 2, 3, 4, 5, 6, 7, 8, and 9 | | All items performed |  |  |