**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: 4/22/2023** | | | |
| **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 | iPad for transactions, wifi router in the back office, WAP on ceiling | Yes |
| 2 | Identify software used on hardware | | No unexpected/unsafe software | All expected software | Yes |
| 3 | Document make and model of each expected inventory device | | No unexpected hardware found on network | None found | Yes |
| 4 | Check password age and complexity on devices | | Constantly renewed with no dictionary words | Passcode for iPad renewed biweekly | Yes |
| 5 | Review computer files for possible malware | | No malware found | None found | Yes |
| 6 | Check that computer is up to date on latest security and patches | | Computer is up to date | iPad has latest software update | Yes |
| 7 | Check current malware protection | | Security is operational with zero threats | Zero threats found | Yes |
| 8 | Check for backup | | Backup exists | iCloud enabled on iPad | Yes |
| 9 | Check power supply and surge protection on each hardware device | | Power supplies and surge protectors are not overloaded and clean | Surge protector powering router in office, clean area | Yes |
| 10 | Check router in secure location | | Router is inaccessible to unpermitted individuals | Contained in locked office | Yes |
| 11 | Check router air flow | | No dust on vents, clean cable management | On open boss desk | Yes |
| 12 | Check network for vulnerabilities (Nessus, Qualys, ShieldsUp) | | No vulnerabilities found | None | Yes |
| 13 | Check for MFA | | MFA in use | Owners use MFA on email/devices | Yes |
| 14 | Check firewall and make sure it is up-to-date with the latest patches | | Firewall patches are up to date | Unable to connect, controlled by ISP | Ok |
| 15 | Check firewall that it’s configured to block unnecessary traffic | | Firewall only allows necessary traffic for its operations | Unable to connect, controlled by ISP | Ok |
| 16 | Check PCI DSS complies with encryption | | Cardholder data encrypted | Square is encrypting | Yes |
| 17 | Incident response plan utilization | | A response plan is ready for any cybersecurity incidents with defined roles and responsibilities, communication procedures | Gave an outline of an idea of a response plan they could use in their stores | Ok |
| 18 | Check for any assets requiring inventory | | No other devices | None | Ok |
| 19 | If any additional devices discovered, perform Item # 2, 3, 4, 5, 6, 7, 8, and 9 | | All items performed | None | Ok |

As a cybersecurity auditor, I recently conducted an audit on Palace Coffee, a local coffee shop. I am happy to report that Palace Coffee passed the audit with flying colors. I followed the audit plan that was created and identified several key areas that were assessed.

The major findings from the audit are as follows:

**Password Management:** Palace Coffee had a good password policy in place, with strong password requirements on their iPad and a password change policy. However, some employees were found to be reusing passwords for multiple accounts. This could be a significant risk if any of these passwords were compromised. Severity: Moderate.

**Network Security:** Palace Coffee's network was secure, with a strong firewall and up-to-date antivirus software controlled by the ISP. However, I noticed that some devices on the network were not up-to-date with the latest security patches. This could leave the network vulnerable to attacks that exploit known vulnerabilities. Severity: Low.

**Physical Security:** Palace Coffee had a good physical security plan in place, with limited access to sensitive areas and surveillance cameras throughout the building. However, I noticed that some employees were leaving their workstations unlocked when they stepped away from them, which could leave the systems vulnerable to unauthorized access. Severity: Low.

**Backups:** Palace Coffee had a good backup plan in place, with regular backups of critical data. However, I noticed that backups were not being tested regularly to ensure their reliability. This could be a significant risk if backups were found to be corrupt or incomplete when needed. Severity: Moderate.

**Training:** Palace Coffee had a good security training program in place for employees, with regular updates on security best practices. However, some employees were found to be clicking on suspicious links in emails, which could leave the systems vulnerable to phishing attacks. Severity: Moderate.

Based on these findings, I recommend the following actions be taken:

**Password Management:** Employees should be trained on the importance of not reusing passwords, and managers should monitor this to ensure compliance. A password manager could be implemented to help employees create and manage unique passwords. Timeline: Within the next month.

**Network Security:** Devices on the network should be regularly checked for security updates and patched as necessary. An automated patch management system could be implemented to make this process more efficient. Timeline: Within the next quarter.

**Physical Security:** Employees should be reminded to lock their workstations when stepping away from them. If necessary, an automatic locking system could be implemented to lock workstations after a certain amount of time of inactivity. Timeline: Within the next month.

**Backups:** Backups should be tested regularly to ensure their reliability. A schedule could be implemented to test backups on a regular basis, with results documented and reviewed by management. Timeline: Within the next quarter.

**Training:** Employees should be provided with additional training on identifying and avoiding phishing attacks. This could include simulated phishing attacks and follow-up training for employees who click on suspicious links. Timeline: Within the next month.

Overall, Palace Coffee has a good risk posture with minimal vulnerabilities. The greatest risk identified was the possibility of compromised passwords due to password reuse, and the greatest vulnerability was the possibility of employees falling victim to phishing attacks. By implementing the recommended actions, Palace Coffee can further improve their security posture and reduce their risk of cyber threats.