**Audit Plan for a Church in Marana-Tucson , Arizona**

**Purpose**

The purpose of this audit is to audit a small church’s cybersecurity

**Outcome**

The outcome of this audit will be recommendations for the church on its cybersecurity

**Scope**

The scope of the audit is the physical accesses, security cameras, Internet connection, computer, and data processes such as live church streaming and management of website tithe payment and donations.

**Audit Procedure**

**Arrival**: The auditor will arrive at the church premises after church service on a Sunday and contact the church’s IT personnel lead and Pastor Lynn for an access authorization to proceed. Auditor will then walk into the facility to gauge the staff reaction.

**Introduction**: Once auditor is satisfied with the entry exercise I will introduce myself to the church IT lead and the members of the IT team.

**Audit Meeting**: Once introduced, the auditor will work with the church IT and any members of the staff, as requested by Pastor Lynn, to complete the attached audit plan documentation. Items may be added to the audit plan as necessary and as agreed between the auditor and the IT team.

**Audit Hot Wash**: Once the auditor and the IT team Lead has completed the attached Audit Plan document the auditor/audit team will inform the IT team that the audit is complete and will then conduct a post audit meeting with other IT team members and the Pastor. The purpose of this meeting will be for the auditor to convey initial findings and for the auditor, IT team and Pastor to generate and agree on any needed action plan.

**Audit Commenced (time/date):** 11/10/2024 at 9:45am **Audit Complete (time/date):** 11/10/2024 at 10:15am

**Auditor:**

Godfred Amponsah

**(Put contact name here):**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | | **Audit Plan:**  **Items and Observations**  **Auditor: Godfred Amponsah Date:11/10/2024** | | | |
| **Item #** | **Description** | | **Expected Findings / Pass Criteria** | **Observations** | **Pass (Yes/No)** |
| 1 | **Review Password Policies for Church Systems** | | Strong, complex passwords in use; no default or weak passwords | Some weak passwords like "Marana\_Methodist" found | No |
| 2 | **Assess Access Control for Admin Accounts** | | Limited access to only authorized personnel | Multiple staff have admin access; need role-based control | No |
| 3 | **Check Website Security (SSL Certificate)** | | Website should have active SSL/TLS encryption (HTTPS) | SSL certificate active and up to date; secure connection noted | Yes |
| 4 | **Examine Online Payment Security** | | Payments secured with PCI-compliant processor; 2FA enabled | PCI-compliant processor in use; no 2FA for admin dashboard | No |
| 5 | **Verify Backup Procedures for Website and Financial Data** | | Regular backups of data; stored securely on cloud or external drives | Backups are regular but stored only on a local drive | No |
| 6 | **Test Firewall and Network Security** | | Firewall active, strong network security measures in place | Basic firewall settings; needs configuration review | No |
| 7 | **Check for Missing System and Website Updates** | | All systems and plugins should be up to date | WordPress plugins outdated; security patches pending | No |
| 8 | **Review Anti-Malware Software** | | Active and updated malware protection | Anti-malware software installed but last updated 6 months ago | No |
| 9 | **Ensure Website Vulnerability Scanning** | | Regular scans for vulnerabilities and threats | No vulnerability scans conducted in the last year | No |
| 10 | **Inspect Security of Online Streaming Platform** | | Secure login, limited access, no public admin URLs | Admin access URL publicly visible; requires stronger login | No |
| 11 | **Assess Data Encryption for Donation Information** | | All sensitive data (e.g., payment info) should be encrypted | Payment data encrypted during transmission | Yes |
| 12 | **Check Email Security for Phishing Protection** | | Anti-phishing measures in place; awareness training conducted | No anti-phishing training or email filters in place | No |
| 13 | **Evaluate Physical Security of IT Equipment** | | Equipment in secure, controlled-access areas | Office left unlocked; equipment accessible by anyone | No |
| 14 | **Verify Use of Multi-Factor Authentication (MFA)** | | MFA enabled for all critical accounts | MFA active for financial accounts; missing for staff emails | No |
| 15 | **Review Security of Wi-Fi Network** | | Wi-Fi should have WPA3 encryption and a strong password | WPA2 encryption used; guest network unsecured | No |
| 16 | **Check Incident Response Plan** | | A clear, documented plan for handling security breaches | No incident response plan in place | No |
| 17 | **Audit User Permissions for Streaming and Website Access** | | User permissions aligned with role-based access control | All users have similar permissions; requires role segregation | No |
| 18 | **Verify Website Uptime Monitoring and Alerts** | | Uptime monitoring system active; alerts set for downtime | Monitoring active but no alert system in place | No |
| 19 | **Test Payment Processing System's Fraud Detection** | | Fraud detection measures in place; alerts for unusual activity | Basic fraud detection active; needs configuration review | Yes |
| 20 | **Check Social Media Security Measures** | | Accounts secured with strong passwords; limited admin access | Strong passwords; no MFA for social media accounts | No |
| 21 | **Check for security plan** | | A clear, documented security plan outlining role, responsibilities, incident response, and periodic review | No formal security plan or documentation exists | No |