**Audit Plan – Lucifer Lighting**

**Purpose**

The purpose of this audit is to check the configuration and security of the computer server and router at a lighting manufacturing company, Lucifer Lighting. This was a previous employer so they are willing to work with me for this assignment. I stay in contact with many of the employees. As the firm’s main focus is design engineering, cybersecurity and protection of their CAD based designs is of upmost importance. While reviewing the security of the computer systems, the physical security and security processes of the manufacturing buildings will also be reviewed for comments.

**Outcome**

The outcome of this audit will be recommendations for the owner of the manufacturing firm and IT manager.

**Scope**

The scope of the audit is the computer engineering server and data processes for storage and backup.

**Audit Procedure**

**Arrival and Introduction**: The auditor will arrive at the facility and contact the IT manager, Hector Green, for authorization to proceed as permission was already granted by leadership. After a brief walkthrough of the facility, the group with introduce themselves to the facility manager, Dave Nosal, who will then join the audit group for this exercise.

**Audit Meeting**: Once the initial steps are completed, the auditor team will work with the IT department members and any members of the staff, as requested by the facility manager, to complete the attached audit plan documentation and make notes for any additions. Any additions will be documented using the blank lines in the audit plan.

**Audit Hot Wash**: Once the auditor team has completed the attached Audit Plan document, the auditor will inform the CEO that the audit is completed and then compile a document with all the results for their review, and if available, hold a post audit meeting. The purpose of this document and potential meeting will be for the auditor team to discuss their findings and recommend to leadership any needed action plan which should be put in place to resolve any alarming findings.

**Audit Planned Day and time: 9:00AM, 11/14/2022**

**Audit Tentative Completed day and time: 11:00AM, 11/14/2022**

**Auditor team:** Megan Moore, Hector Green, Dave Nosal

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | | **Audit Plan:**  **Items and Observations**  **Auditor: Date:** | | | |
| **Item #** | **Description** | | **Expected Findings/pass criteria** | **Observations** | **Pass (Yes/No)** |
| 1 | Check network password strength | | Should be strong: no dictionary word |  |  |
| 2 | Check ports using shield’s up | | Ports are in stealth or at least closed |  |  |
| 3 | Check for missing updates; versions of software | | Computer is up to date with auto updates on |  |  |
| 4 | Cloud backup system in place | | Back up exists; functioning correctly |  |  |
| 5 | Server is kept in a location with controlled access | | Access is limited to those with a need |  |  |
| 6 | Review computer system files for possible malware | | No malware found; antivirus software in place |  |  |
| 7 | Check for access control settings for server | | Only IT manager or department can access all files |  |  |
| 8 | Check for surge protection on power supply | | Surge protection present |  |  |
| 9 | Check server and router in location with temp control and good air flow | | Air flow and temperature in acceptable range |  |  |
| 10 | Ensure router is password protected | | Password is active |  |  |
| 11 | Ensure access controlled on all business systems with user profiles | | Access is controlled; all users assigned profiles |  |  |
| 12 | Ask about a security plan | | Security policies are in place |  |  |
| 13 | Building security | | Is there protocol in place for theft; insurance policy coverage |  |  |