# Controls and compliance checklist

| Yes | No | Control |
|---|---|---|
| ☐ | ☑ | Least Privilege Least Privilege (The company has mechanisms to reduce risks, but it needs to improve the safety of assets management and be fully in line with safety standards) |
| ☐ | ☑ | Disaster recovery plans (There are no disaster recovery plans in place. These need to be implemented to ensure business continuity). |
| ☐ | ☑ | Password policies (Password policy exists, but it does not meet the minimum requirements) |
| ☐ | ☑ | Separation of duties (has to be implemented to reduce risk and overall impact of malicious insider or compromised accounts) |
| ☑ | ☐ | Firewall |
| ☑ | ☐ | Intrusion detection system (IDS) (IDS has not been instaled yet, it is necessary to to detect and prevent anomalous traffic). |
| ☐ | ☑ | Backups (The IT department needs to have backups of critical data, in the case of restore/recovering from an event). |
| ☑ | ☐ | Antivirus software |
| ☐ | ☑ | Manual monitoring, maintenance, and intervention for legacy systems (there is no regular schedule in place for these tasks and intervention methods are unclear). |
| ☐ | ☑ | Encryption (Encryption is not currently used, has to be implemented to ensure credibility of customers) |
| ☐ | ☑ | Password management system (There is no centralized password management system, which means that is a affecting productivity) |
| ☑ | ☐ | Locks (offices, storefront, warehouse) |
| ☑ | ☐ | Closed-circuit television (CCTV) surveillance |

| | | |
|---|---|---|
| ☑ | ☐ | Fire detection/prevention (fire alarm, sprinkler system, etc.) |

---

**Compliance checklist**

Payment Card Industry Data Security Standard (PCI DSS)

| Yes | No | Best practice |
|---|---|---|
| ☐ | ☑ | Only authorized users have access to customers' credit card information. (Currently, all employees have access to the company's internal data). |
| ☐ | ☑ | Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment. (it is not a secure environment because all employees have access) |
| ☐ | ☑ | Implement data encryption procedures to better secure credit card transaction touchpoints and data. (The company does not currently use encryption to ensure the confidentiality of customers' financial information). |
| ☐ | ☑ | Adopt secure password management policies. (Password policies are nominal and no password management system is currently in place). |

General Data Protection Regulation (GDPR)

| Yes | No | Best practice |
|---|---|---|
| ☐ | ☑ | E.U. customers' data is kept private/secured. (The IT department has established a plan to notify E.U. customers within 72 hours if there is a security breach. However, there is a lack of cryptography and password minimum requirements). |
| ☑ | ☐ | There is a plan in place to notify E.U. customers within 72 hours if |

their data is compromised/there is a breach.

| | | |
|---|---|---|
| ☐ | ☑ | Ensure data is properly classified and inventoried. (Currently, there is inadequate management of assets). |
| ☐ | ☐ | Enforce privacy policies, procedures, and processes to properly document and maintain data. |

System and Organizations Controls (SOC type 1, SOC type 2)

| Yes | No | Best practice |
|---|---|---|
| ☐ | ☑ | User access policies are established. (Controls of Least Privilege and separation of duties are not currently in place; all employees have access to internally stored data). |
| ☐ | ☑ | Sensitive data (PII/SPII) is condential/private. (Currently, all employees have access to internally stored data and may be able to access cardholder data and customers' PII/SPII, for this reason it is not secure. |
| ☑ | ☐ | Data integrity ensures the data is consistent, complete, accurate, and has been validated. |
| ☐ | ☑ | Data is available to individuals authorized to access it. (Data is available to all employees, and needs to be limited to only the individuals who need access to it to do their jobs). |