**Control Assessment Checklist:**

| **Control** | **Yes** | **No** | **Explanation** |
| --- | --- | --- | --- |
| Least Privilege |  | No | All employees have access to customer data; privileges need to be limited. |
| Disaster Recovery Plans |  | No | No disaster recovery plans are in place. |
| Password Policies |  | No | Employee password requirements are minimal. |
| Separation of Duties |  | No | Needs to be implemented to reduce the possibility of fraud/access to critical data. |
| Firewall | Yes |  | Existing firewall blocks traffic based on appropriately defined rules. |
| Intrusion Detection System (IDS) |  | No | IDS needs to be implemented. |
| Backups |  | No | Backups of critical data are not in place. |
| Antivirus Software | Yes |  | Antivirus software is installed and monitored regularly. |
| Manual Monitoring, Maintenance, and Intervention for Legacy Systems |  | No | Legacy systems are not on a regular maintenance schedule. |
| Encryption |  | No | Encryption is not currently used. |
| Password Management System |  | No | No password management system is currently in place. |
| Locks (offices, storefront, warehouse) | Yes |  | Physical locations have sufficient locks. |
| Closed-circuit Television (CCTV) Surveillance | Yes |  | CCTV is installed and functioning. |
| Fire Detection/Prevention | Yes |  | Fire detection and prevention systems are in place. |

**Compliance Checklist (PCI DSS):**

| **Best Practice** | **Yes** | **No** | **Explanation** |
| --- | --- | --- | --- |
| Authorized users have access to customers’ credit card information |  | No | Currently, all employees have access to internal data. |
| Credit card information is accepted, processed, transmitted, and stored internally in a secure environment |  | No | Credit card information is not encrypted and all employees currently have access to internal data. |
| Implement data encryption procedures to better secure credit card transaction touchpoints and data |  | No | Data encryption procedures should be implemented. |
| Adopt secure password management policies |  | No | Password policies are nominal, and no password management system is currently in place. |

**Compliance Checklist (GDPR):**

| **Best Practice** | **Yes** | **No** | **Explanation** |
| --- | --- | --- | --- |
| E.U. customers' data is kept private/secured |  | No | The company does not currently use encryption to ensure the confidentiality of customers’ financial information. |
| There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach | Yes |  | A plan is in place to notify E.U. customers within 72 hours of a data breach. |
| Enforce privacy policies, procedures, and processes to properly document and maintain data | Yes |  | Privacy policies, procedures, and processes have been developed and enforced among IT team members and other employees as needed. |

**Compliance Checklist (SOC Type 1, SOC Type 2):**

| **Best Practice** | **Yes** | **No** | **Explanation** |
| --- | --- | --- | --- |
| User access policies are established |  | No | 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 confidential/private |  | No | Encryption is not currently used to ensure the confidentiality of PII/SPII. |
| Data integrity ensures the data is consistent, complete, accurate, and has been validated | Yes |  | Data integrity is in place. |
| Data is available to individuals authorized to access it |  | No | While data is available to all employees, authorization needs to be limited to only the individuals who need access to do their jobs. |