**Controls Assessment Checklist**

| **Control** | **Yes** | **No** |
| --- | --- | --- |
| Least Privilege |  | ● |
| Disaster recovery plans | ● | ● |
| Password policies | ● | ● |
| Separation of duties | ● | ● |
| Firewall | ● | ● |
| Intrusion detection system (IDS) |  | ● |
| Backups | ● | ● |
| Antivirus software | ● | ● |
| Manual monitoring, maintenance, and intervention for legacy systems | ● | ● |
| Encryption |  | ● |
| Password management system | ● | ● |
| 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)**

| **Best Practice** | **Yes** | **No** |
| --- | --- | --- |
| Only authorized users have access to customers’ credit card information. |  | ● |
| Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment. | ● | ● |
| Implement data encryption procedures to better secure credit card transaction touchpoints and data. |  | ● |
| Adopt secure password management policies. | ● | ● |

**General Data Protection Regulation (GDPR)**

| **Best Practice** | **Yes** | **No** |
| --- | --- | --- |
| E.U. customers’ data is kept private/secured. | ● | ● |
| 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. | ● | ● |
| Enforce privacy policies, procedures, and processes to properly document and maintain data. | ● | ● |

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

| **Best Practice** | **Yes** | **No** |
| --- | --- | --- |
| User access policies are established. | ● | ● |
| Sensitive data (PII/SPII) is confidential/private. | ● | ● |
| Data integrity ensures the data is consistent, complete, accurate, and has been validated. | ● | ● |
| Data is available to individuals authorized to access it. | ● | ● |

**Recommendations (Optional)**

* **Implement Least Privilege**: Reduce risk and overall impact of malicious insider or compromised accounts.
* **Install IDS**: Detect and prevent anomalous traffic that matches a signature or rule.
* **Implement Encryption**: Provide confidentiality to sensitive information.
* **Develop Disaster Recovery Plans**: Ensure business continuity.
* **Adopt Secure Password Management Policies**: Reduce likelihood of account compromise through brute force or dictionary attack techniques.
* **Establish User Access Policies**: Bolster confidentiality and integrity by defining which groups can access or modify data.