# Controls Assessment Checklist

|  |  |  |
| --- | --- | --- |
| Control | In Place? | Notes |
| Least Privilege | No | All employees currently have access to internal data, including cardholder and PII data. |
| Disaster recovery plans | No | No disaster recovery plans or backups of critical data are in place. |
| Password policies | No | Password policy exists but is nominal and does not meet current complexity standards. |
| Separation of duties | No | Separation of duties has not been implemented. |
| Firewall | Yes | Firewall is in place with defined security rules. |
| Intrusion detection system (IDS) | No | IDS has not been installed. |
| Backups | No | No backups of critical data exist. |
| Antivirus software | Yes | Antivirus software is installed and monitored regularly. |
| Manual monitoring, maintenance, and intervention for legacy systems | No | Legacy systems are monitored but without a regular schedule or clear intervention methods. |
| Encryption | No | No encryption is used for credit card or sensitive customer data. |
| Password management system | No | No centralized password management system exists. |
| Locks (offices, storefront, warehouse) | Yes | Physical locks are sufficient. |
| Closed-circuit television (CCTV) surveillance | Yes | CCTV surveillance is up-to-date and functioning. |
| Fire detection/prevention (fire alarm, sprinkler system, etc.) | Yes | Fire detection and prevention systems are functioning. |