**Controls and Compliance Checklist**

**1. Controls Assessment Checklist**

| **No.** | **Control** | **Status (Y/N)** |
| --- | --- | --- |
| 1 | Least Privilege | [N] |
| 2 | Disaster Recovery Plans | [N] |
| 3 | Password Policies | [Y] |
| 4 | Separation of Duties | [N] |
| 5 | Firewall | [Y] |
| 6 | Intrusion Detection System (IDS) | [N] |
| 7 | Backups | [N] |
| 8 | Antivirus Software | [Y] |
| 9 | Manual Monitoring, Maintenance, and Intervention for Legacy Systems | [Y] |
| 10 | Encryption | [N] |
| 11 | Password Management System | [N] |
| 12 | Locks (Offices, Storefront, Warehouse) | [Y] |
| 13 | Closed-Circuit Television (CCTV) Surveillance | [Y] |
| 14 | Fire Detection/Prevention (Fire Alarm, Sprinkler System, etc.) | [Y] |

**Notes on Controls**

* **Least Privilege & Separation of Duties**:  
  The audit report indicates that all employees currently have wide access. These controls are not implemented.
* **Disaster Recovery Plans & Backups**:  
  No formal disaster recovery plans or backup processes are in place.
* **Password Policies vs. Password Management System**:  
  There is a minimal password policy, but no centralized system to enforce robust requirements.
* **Encryption & IDS**:  
  Encryption is not used for sensitive payment data, and there is no Intrusion Detection System (IDS) installed.
* **Other Controls**:  
  Firewall, antivirus software, manual monitoring, physical locks, CCTV, and fire detection/prevention systems are in place.

**2. Compliance Checklist**

**2.1 Payment Card Industry Data Security Standard (PCI DSS)**

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

**Notes (PCI DSS):**  
The current environment allows broad access to sensitive cardholder data, lacks encryption, and uses a nominal password policy that does not meet secure standards.

**2.2 General Data Protection Regulation (GDPR)**

| **Yes/No** | **Best Practice** |
| --- | --- |
| [N] | EU customers’ data is kept private and secured. |
| [Y] | A plan is in place to notify EU customers within 72 hours if data is compromised or there is a breach. |
| [N] | Data is properly classified and inventoried. |
| [Y] | Privacy policies, procedures, and processes are enforced to properly document and maintain data. |

**Notes (GDPR):**  
Although the company has a breach notification plan and enforces privacy policies, access to data is not strictly restricted, and asset classification/inventory is lacking.

**2.3 System and Organization Controls (SOC Type 1, SOC Type 2)**

| **Yes/No** | **Best Practice** |
| --- | --- |
| [N] | New user access policies are established. |
| [N] | Sensitive data (PII/SPII) is confidential/private. |
| [Y] | Data integrity ensures the data is accurate, consistent, and validated. |
| [N] | Data is available only to individuals authorized to access it. |

**Notes (SOC):**  
While technical controls ensure data integrity, the lack of proper user access restrictions means data is too broadly available.

**3. Recommendations**

**For the IT Manager:**

1. **Implement Access Controls**
   * Establish and enforce least privilege and separation of duties to ensure that only authorized personnel can access sensitive data.
2. **Develop Disaster Recovery & Backup Strategies**
   * Create formal disaster recovery plans.
   * Schedule regular backups of critical data to mitigate data loss risks.
3. **Enhance Password & Encryption Policies**
   * Update the password policy to meet current industry standards.
   * Deploy a centralized password management system.
   * Implement encryption for sensitive data, especially for credit card transactions.
4. **Deploy Additional Monitoring Tools**
   * Install an Intrusion Detection System (IDS) to detect anomalous network traffic and potential threats.
5. **Review Compliance Gaps**
   * Address identified PCI DSS and GDPR non-compliances by refining user access controls and securing data storage, processing, and transmission.