# Compliance Checklist

|  |  |  |
| --- | --- | --- |
| Compliance Best Practice | In Place? | Notes |
| Only authorized users have access to customers’ credit card information | No | All employees have access to cardholder data. |
| Credit card information is stored, accepted, processed, and transmitted internally in a secure environment | No | No encryption or adequate controls for cardholder data. |
| Implement data encryption procedures to better secure credit card transaction touchpoints and data | No | Encryption is not currently implemented. |
| Adopt secure password management policies | No | Password policies are weak and no centralized management system exists. |
| E.U. customers’ data is kept private/secured | Yes | Privacy policies and procedures are in place and enforced. |
| There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach | Yes | Notification plan exists. |
| Ensure data is properly classified and inventoried | No | Asset management and classification are inadequate. |
| Enforce privacy policies, procedures, and processes to properly document and maintain data | Yes | Policies and procedures are enforced. |
| User access policies are established | No | Access controls such as least privilege and separation of duties are not implemented. |
| Sensitive data (PII/SPII) is confidential/private | No | Lack of encryption and access controls puts sensitive data at risk. |
| Data integrity ensures the data is consistent, complete, accurate, and has been validated | Yes | Availability and integrated controls are in place to ensure data integrity. |
| Data is available to individuals authorized to access it | Yes | Access is available but not properly restricted. |