SaaS Card Storage Compliance Checklist

Use this checklist to audit your current payment infrastructure and ensure your storage methods align with the latest security standards.

Phase 1: Compliance & Strategy Assessment

- [ ] Identify your current PCI DSS compliance level based on your annual transaction volume.
- [ ] Verify that you have completed the relevant Self-Assessment Questionnaire (SAQ) for your integration type.
- [ ] Confirm that your business does not store full 16-digit card numbers in plain text on any local server or database.
- [ ] Audit your current software stack to ensure no cardholder data is being saved within your CRM or helpdesk tools.
- [ ] Evaluate the cost of your current security maintenance versus the benefits of switching to a Merchant of Record model.

Phase 2: Technical Implementation & Automation

- [ ] Replace all raw card entries with unique tokens provided by your payment processor.
- [ ] Implement a hosted checkout or iframe to ensure sensitive data bypasses your web server entirely.
- [ ] Enable an automated card updater service to sync expired or replaced credentials with card networks.
- [ ] Configure your billing logic to automatically retry failed transactions before triggering a service suspension.

- [ ] Verify that your system uses AES 256-bit encryption for any non-sensitive customer identifiers stored locally.
- [ ] Test your tokenization API to ensure it correctly returns tokens without exposing raw data in server logs.

Phase 3: Access Control & Internal Security

- [ ] Mandate Multi-Factor Authentication (MFA) for every team member with access to the billing dashboard.
- [ ] Assign unique login IDs to all employees to create a clear audit trail of data access.
- [ ] Review employee permissions and revoke "Export" or "View" privileges for anyone whose role does not strictly require them.
- [ ] Establish a quarterly review process to remove access for former employees or those who have changed departments.
- [ ] Conduct a scan of your internal communication channels like Slack or Email to ensure no staff are sharing card details manually.

Phase 4: Data Retention & Disposal

- [ ] Set up an automated script to permanently delete CVV/CVC codes immediately after transaction authorization.
- [ ] Define a clear retention period for payment tokens, such as twelve months after a subscription is cancelled.
- [ ] Implement a "Secure Wipe" protocol for any legacy hardware or cloud storage used for backup payment data.
- [ ] Draft a formal data disposal policy and share it with your engineering and compliance teams.
- [ ] Schedule a biannual "Data Cleanup Day" to purge inactive customer records and minimize your breach surface area.